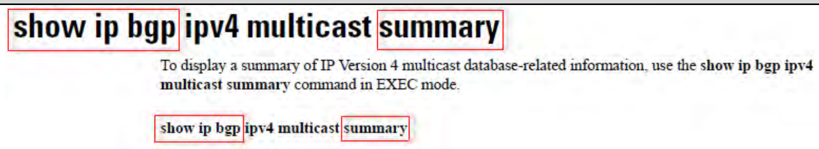
<table>
<tr><th>Copyright Registration Information</th><th>Cisco</th><th>Arista</th></tr>
<tr>
<td>Cisco IOS 15.4

Effective date of registration: 11/26/2014</td>
<td>

show ip bgp ipv4 multicast summary
To display a summary of IP Version 4 multicast database-related information, use the show ip bgp ipv4 multicast summary command in EXEC mode.
show ip bgp ipv4 multicast summary

Cisco IOS IP Routing: BGP Command Reference (2013), at 757

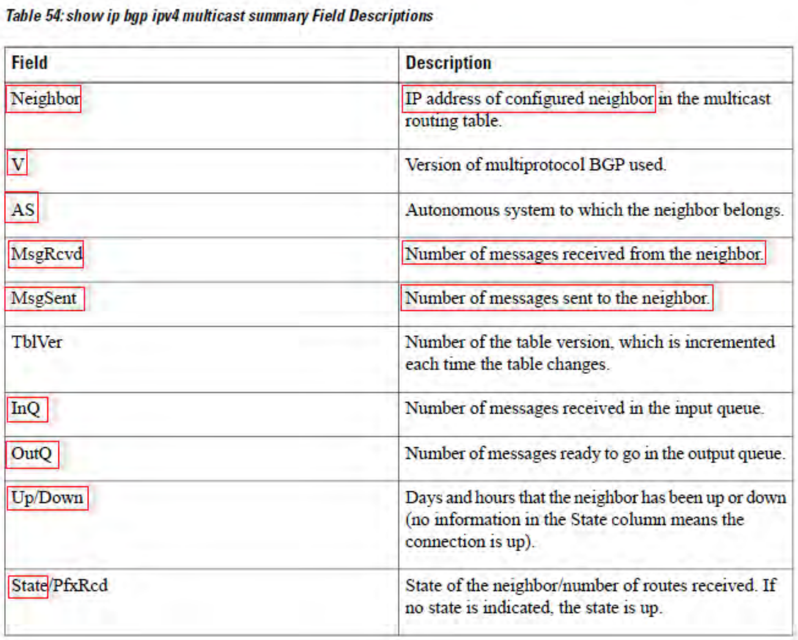
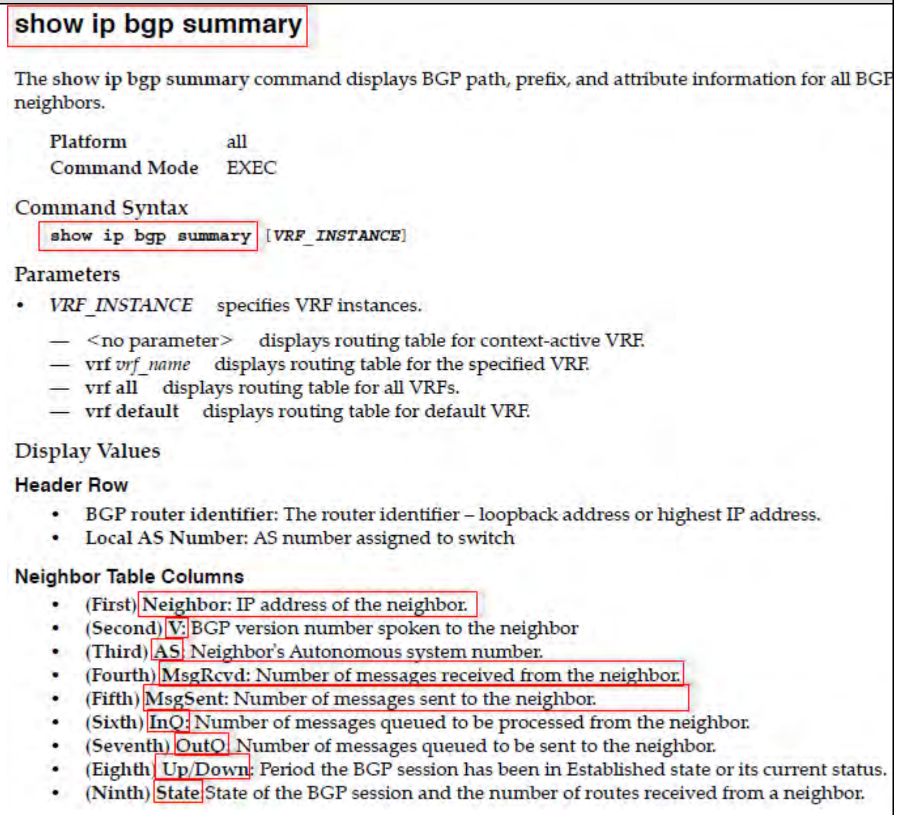


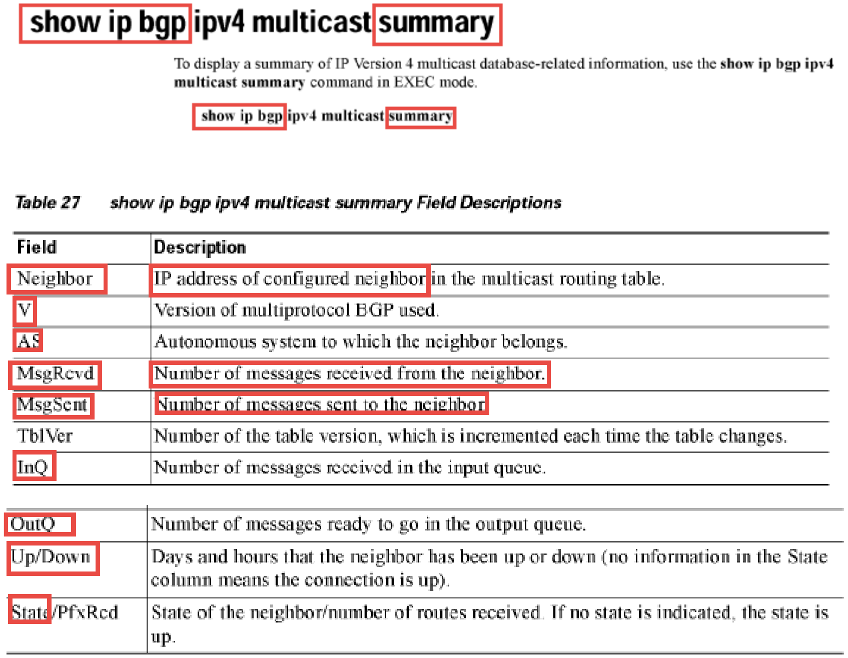
Table 54: show ip bgp ipv4 multicast summary Field Descriptions
<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Neighbor</td><td>IP address of configured neighbor in the multicast routing table.</td></tr>
<tr><td>V</td><td>Version of multiprotocol BGP used.</td></tr>
<tr><td>AS</td><td>Autonomous system to which the neighbor belongs.</td></tr>
<tr><td>MsgRcvd</td><td>Number of messages received from the neighbor.</td></tr>
<tr><td>MsgSent</td><td>Number of messages sent to the neighbor.</td></tr>
<tr><td>TblVer</td><td>Number of the table version, which is incremented each time the table changes.</td></tr>
<tr><td>InQ</td><td>Number of messages received in the input queue.</td></tr>
<tr><td>OutQ</td><td>Number of messages ready to go in the output queue.</td></tr>
<tr><td>Up/Down</td><td>Days and hours that the neighbor has been up or down (no information in the State column means the connection is up).</td></tr>
<tr><td>State/PfxRcd</td><td>State of the neighbor/number of routes received. If no state is indicated, the state is up.</td></tr>
</table>

Cisco IOS IP Routing: BGP Command Reference (2013), at 758.
</td>
<td>

show ip bgp summary
The show ip bgp summary command displays BGP path, prefix, and attribute information for all BGP neighbors.
Platform all
Command Mode EXEC
Command Syntax
show ip bgp summary [VRF_INSTANCE]
Parameters
• VRF_INSTANCE specifies VRF instances.
— <no parameter> displays routing table for context-active VRF.
— vrf vrf_name displays routing table for the specified VRF.
— vrf all displays routing table for all VRFs.
— vrf default displays routing table for default VRF.
Display Values
Header Row
• BGP router identifier: The router identifier – loopback address or highest IP address.
• Local AS Number: AS number assigned to switch
Neighbor Table Columns
• (First) Neighbor: IP address of the neighbor.
• (Second) V: BGP version number spoken to the neighbor
• (Third) AS: Neighbor's Autonomous system number.
• (Fourth) MsgRcvd: Number of messages received from the neighbor.
• (Fifth) MsgSent: Number of messages sent to the neighbor.
• (Sixth) InQ: Number of messages queued to be processed from the neighbor.
• (Seventh) OutQ: Number of messages queued to be sent to the neighbor.
• (Eighth) Up/Down: Period the BGP session has been in Established state or its current status.
• (Ninth) State State of the BGP session and the number of routes received from a neighbor.

Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1641.

See also Arista User Manual v. 4.12.3 (7/17/13), at 1407; Arista User Manual, v. 4.11.1 (1/11/13), at 1153; Arista User Manual v. 4.10.3 (10/22/12), at 964; Arista User Manual v. 4.9.3.2 (5/3/12), at 728; Arista User Manual v. 4.8.2 (11/18/11), at 549; Arista User Manual v. 4.7.3 (7/18/11), at 402.
</td>
</tr>
</table>

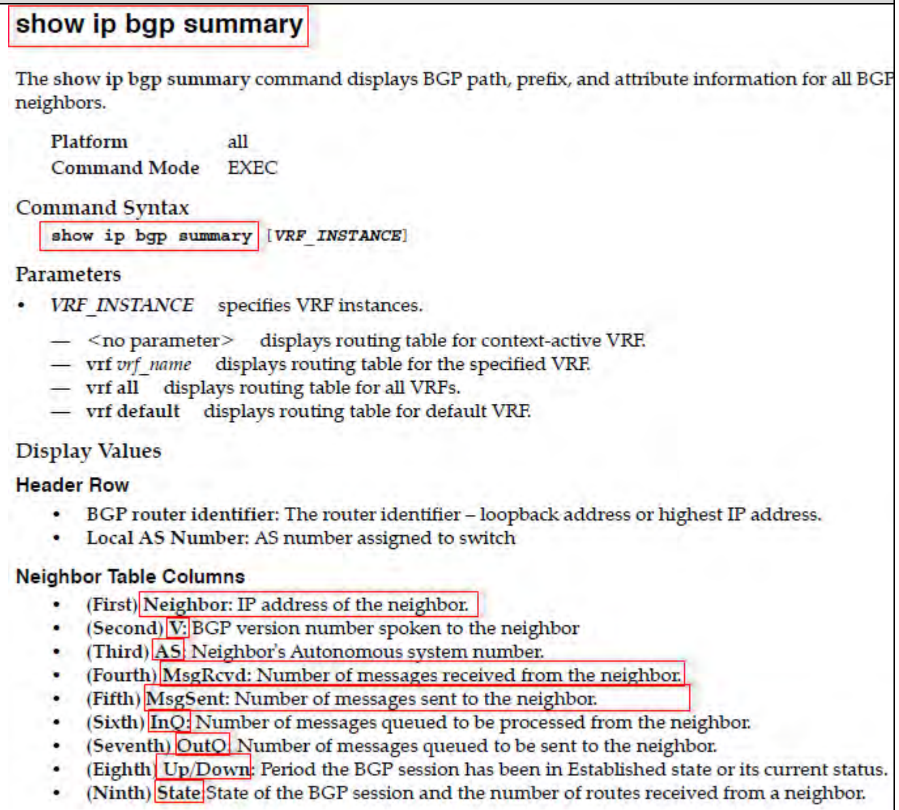
<table>
<tr><th>Copyright Registration Information</th><th>Cisco</th><th>Arista</th></tr>
<tr>
<td>Cisco IOS 12.4

Effective date of registration: 8/12/2005</td>
<td>
show ip bgp ipv4 multicast summary

To display a summary of IP Version 4 multicast database-related information, use the <b>show ip bgp ipv4 multicast summary</b> command in EXEC mode.

<b>show ip bgp ipv4 multicast summary</b>

<i>Table 27 show ip bgp ipv4 multicast summary Field Descriptions</i>
<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Neighbor</td><td>IP address of configured neighbor in the multicast routing table.</td></tr>
<tr><td>V</td><td>Version of multiprotocol BGP used.</td></tr>
<tr><td>AS</td><td>Autonomous system to which the neighbor belongs.</td></tr>
<tr><td>MsgRcvd</td><td>Number of messages received from the neighbor.</td></tr>
<tr><td>MsgSent</td><td>Number of messages sent to the neighbor</td></tr>
<tr><td>TblVer</td><td>Number of the table version, which is incremented each time the table changes.</td></tr>
<tr><td>InQ</td><td>Number of messages received in the input queue.</td></tr>
<tr><td>OutQ</td><td>Number of messages ready to go in the output queue.</td></tr>
<tr><td>Up/Down</td><td>Days and hours that the neighbor has been up or down (no information in the State column means the connection is up).</td></tr>
<tr><td>State/PfxRcd</td><td>State of the neighbor/number of routes received. If no state is indicated, the state is up.</td></tr>
</table>

Cisco IOS IP Routing Protocols Command Reference (June 10, 2005), at 308.</td>
<td>
show ip bgp summary

The show ip bgp summary command displays BGP path, prefix, and attribute information for all BGP neighbors.

Platform all
Command Mode EXEC

Command Syntax
show ip bgp summary [<i>VRF_INSTANCE</i>]

Parameters
• <i>VRF_INSTANCE</i> specifies VRF instances.
— <no parameter> displays routing table for context-active VRF.
— vrf <i>vrf_name</i> displays routing table for the specified VRF.
— vrf all displays routing table for all VRFs.
— vrf default displays routing table for default VRF.

Display Values
Header Row
• BGP router identifier: The router identifier – loopback address or highest IP address.
• Local AS Number: AS number assigned to switch

Neighbor Table Columns
• (First) Neighbor: IP address of the neighbor.
• (Second) V: BGP version number spoken to the neighbor
• (Third) AS: Neighbor's Autonomous system number.
• (Fourth) MsgRcvd: Number of messages received from the neighbor.
• (Fifth) MsgSent: Number of messages sent to the neighbor.
• (Sixth) InQ: Number of messages queued to be processed from the neighbor.
• (Seventh) OutQ: Number of messages queued to be sent to the neighbor.
• (Eighth) Up/Down: Period the BGP session has been in Established state or its current status.
• (Ninth) State State of the BGP session and the number of routes received from a neighbor.

Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1641.

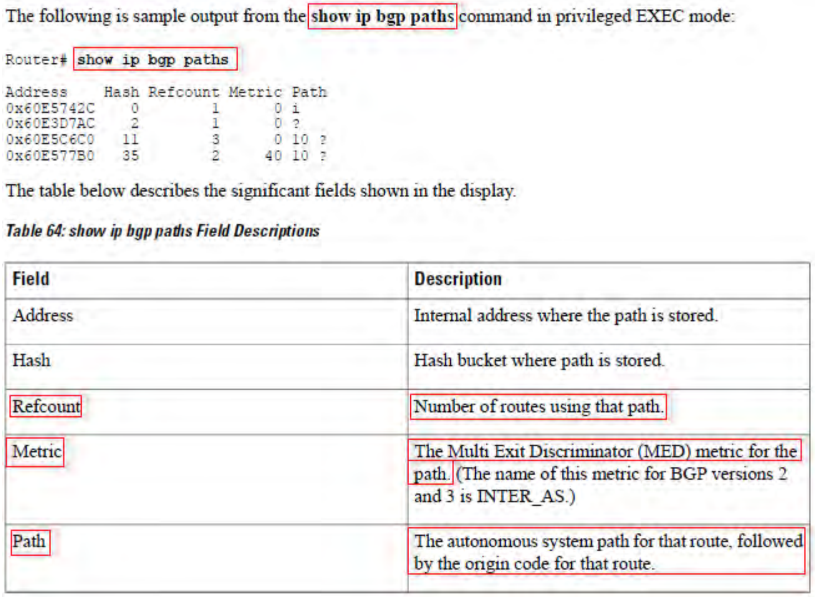
<i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 1407; Arista User Manual, v. 4.11.1 (1/11/13), at 1153; Arista User Manual v. 4.10.3 (10/22/12), at 964; Arista User Manual v. 4.9.3.2 (5/3/12), at 728; Arista User Manual v. 4.8.2 (11/18/11), at 549; Arista User Manual v. 4.7.3 (7/18/11), at 402.</td>
</tr>
</table>

<table>
<tr><th>Copyright Registration Information</th><th>Cisco</th><th>Arista</th></tr>
<tr>
<td>

Cisco IOS 15.4

Effective date of registration: 11/26/2014

</td>
<td>



The following is sample output from the **show ip bgp paths** command in privileged EXEC mode:

```
Router# show ip bgp paths

Address    Hash Refcount Metric Path
0x60E5742C    0        1      0 i
0x60E3D7AC    2        1      0 ?
0x60E5C6C0   11        3      0 10 ?
0x60E577B0   35        2     40 10 ?
```

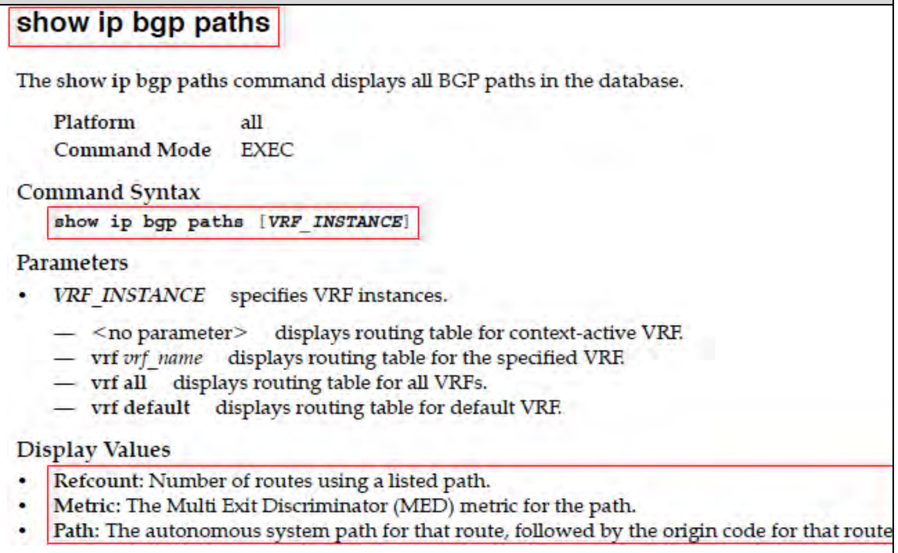
The table below describes the significant fields shown in the display.

Table 64: show ip bgp paths Field Descriptions

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Address</td><td>Internal address where the path is stored.</td></tr>
<tr><td>Hash</td><td>Hash bucket where path is stored.</td></tr>
<tr><td>Refcount</td><td>Number of routes using that path.</td></tr>
<tr><td>Metric</td><td>The Multi Exit Discriminator (MED) metric for the path. (The name of this metric for BGP versions 2 and 3 is INTER_AS.)</td></tr>
<tr><td>Path</td><td>The autonomous system path for that route, followed by the origin code for that route.</td></tr>
</table>

Cisco IOS IP Routing: BGP Command Reference (2013), at 795.

</td>
<td>



show ip bgp paths

The show ip bgp paths command displays all BGP paths in the database.

Platform all
Command Mode EXEC

Command Syntax

```
show ip bgp paths [VRF_INSTANCE]
```

Parameters

- *VRF_INSTANCE* specifies VRF instances.
  - — <no parameter> displays routing table for context-active VRF.
  - — vrf *vrf_name* displays routing table for the specified VRF.
  - — vrf all displays routing table for all VRFs.
  - — vrf default displays routing table for default VRF.

Display Values

- Refcount: Number of routes using a listed path.
- Metric: The Multi Exit Discriminator (MED) metric for the path.
- Path: The autonomous system path for that route, followed by the origin code for that route

Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1638,

See also Arista User Manual v. 4.13.6F (4/14/2014), at 1588; Arista User Manual v. 4.12.3 (7/17/13), at 1405; Arista User Manual, v. 4.11.1 (1/11/13), at 1151; Arista User Manual v. 4.10.3 (10/22/12), at 962; Arista User Manual v. 4.9.3.2 (5/3/12), at 725; Arista User Manual v. 4.8.2 at 547; Arista User Manual v. 4.8.2 (11/18/11), at 547; Arista User Manual v. 4.7.3 (7/18/11), at 401; Arista User Manual v. 4.6.0 (12/22/2010), at 249; Arista User Manual v. 4.6.0 (12/22/2010), at 249

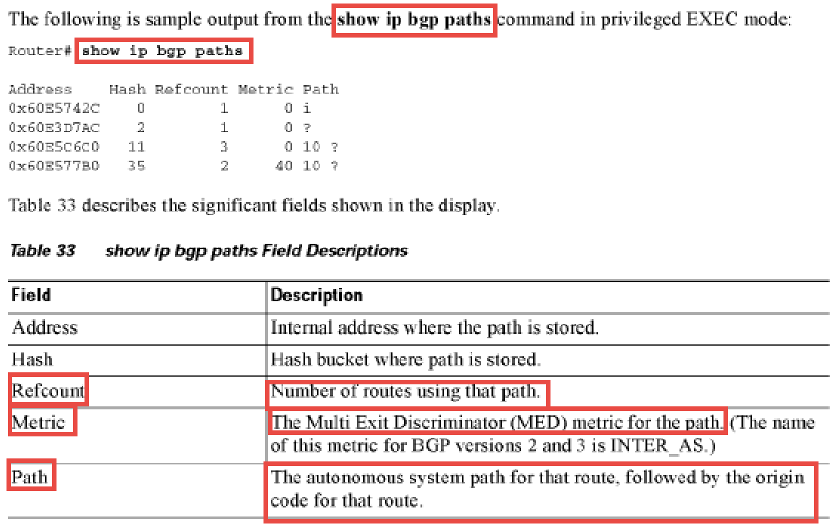
</td>
</tr>
</table>

<table>
<tr><th>Copyright Registration Information</th><th>Cisco</th><th>Arista</th></tr>
<tr>
<td>

Cisco IOS 12.4

Effective date of registration: 8/12/2005

</td>
<td>



The following is sample output from the **show ip bgp paths** command in privileged EXEC mode:

```
Router# show ip bgp paths

Address     Hash Refcount Metric Path
0x60E5742C    0        1      0 i
0x60E3D7AC    2        1      0 ?
0x60E5C6C0   11        3      0 10 ?
0x60E577B0   35        2     40 10 ?
```

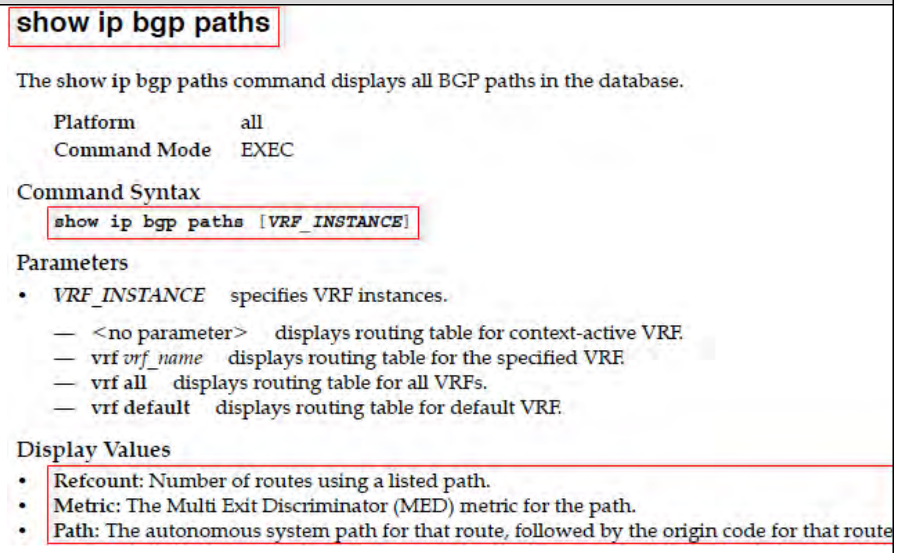
Table 33 describes the significant fields shown in the display.

Table 33   show ip bgp paths Field Descriptions

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Address</td><td>Internal address where the path is stored.</td></tr>
<tr><td>Hash</td><td>Hash bucket where path is stored.</td></tr>
<tr><td>Refcount</td><td>Number of routes using that path.</td></tr>
<tr><td>Metric</td><td>The Multi Exit Discriminator (MED) metric for the path. (The name of this metric for BGP versions 2 and 3 is INTER_AS.)</td></tr>
<tr><td>Path</td><td>The autonomous system path for that route, followed by the origin code for that route.</td></tr>
</table>

Cisco IOS IP Routing Protocols Command Reference (June 10, 2005), at 308.

</td>
<td>



show ip bgp paths

The show ip bgp paths command displays all BGP paths in the database.

Platform all
Command Mode EXEC

Command Syntax

```
show ip bgp paths [VRF_INSTANCE]
```

Parameters

- *VRF_INSTANCE* specifies VRF instances.
  - — <no parameter> displays routing table for context-active VRF.
  - — vrf *vrf_name* displays routing table for the specified VRF.
  - — vrf all displays routing table for all VRFs.
  - — vrf default displays routing table for default VRF.

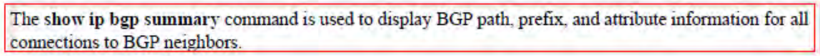
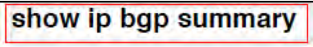
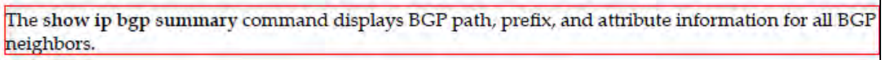
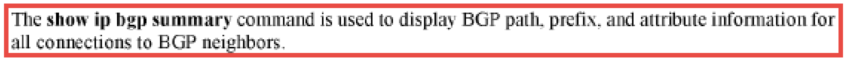
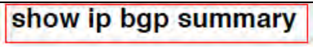
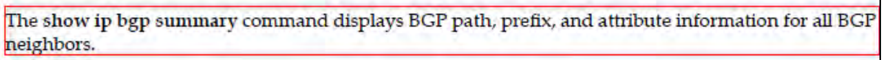
Display Values

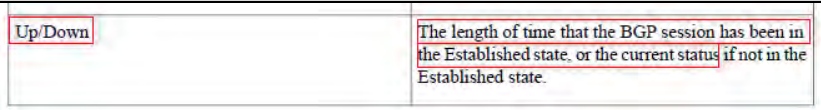
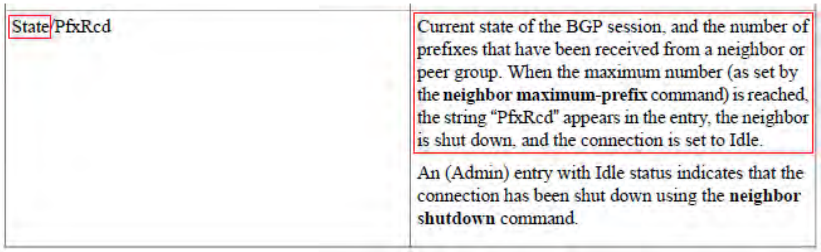
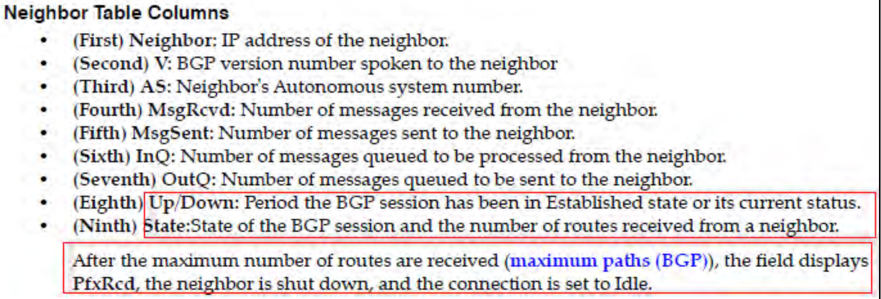
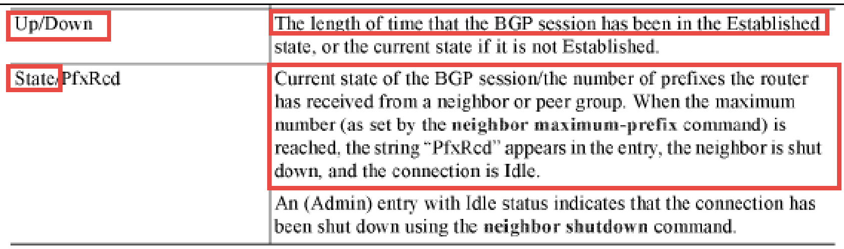
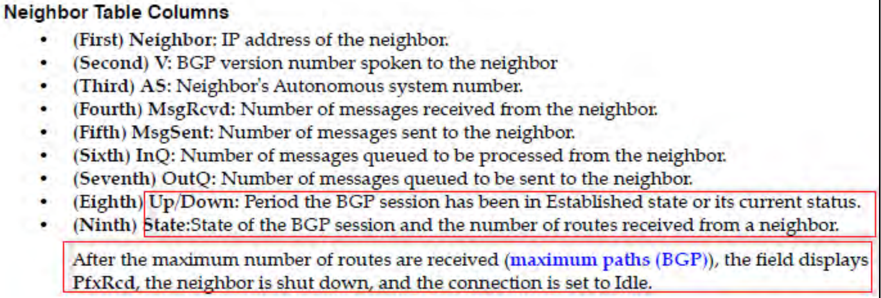
- Refcount: Number of routes using a listed path.
- Metric: The Multi Exit Discriminator (MED) metric for the path.
- Path: The autonomous system path for that route, followed by the origin code for that route

Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1638,

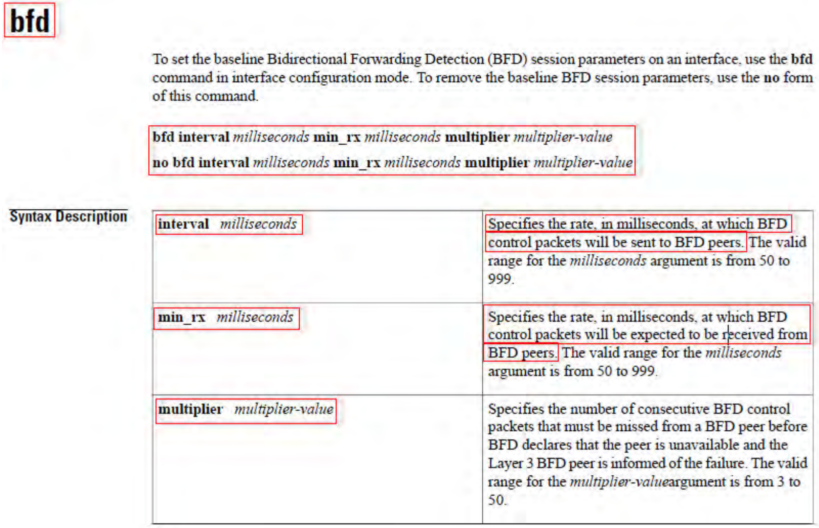
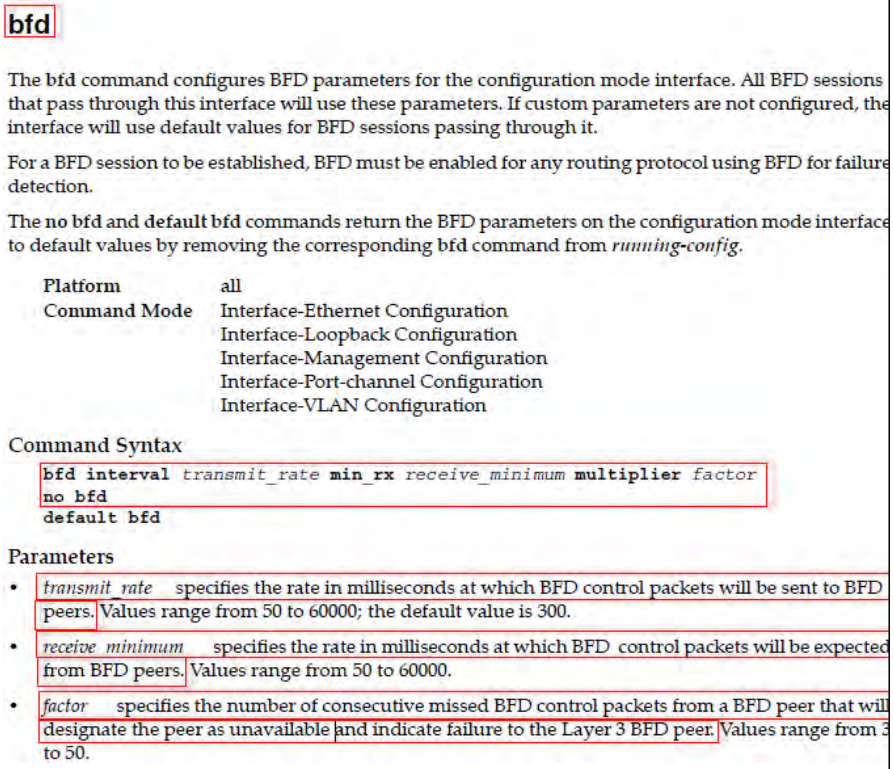
See also Arista User Manual v. 4.13.6F (4/14/2014), at 1588; Arista User Manual v. 4.12.3 (7/17/13), at 1405; Arista User Manual, v. 4.11.1 (1/11/13), at 1151; Arista User Manual v. 4.10.3 (10/22/12), at 962; Arista User Manual v. 4.9.3.2 (5/3/12), at 725; Arista User Manual v. 4.8.2 at 547; Arista User Manual v. 4.8.2 (11/18/11), at 547 ; Arista User Manual v. 4.7.3 (7/18/11), at 401; Arista User Manual v. 4.6.0 (12/22/2010), at 249; Arista User Manual v. 4.6.0 (12/22/2010), at 249

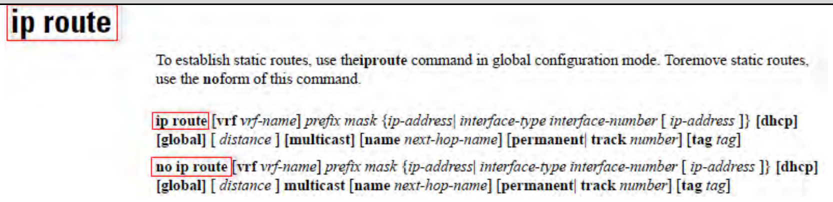
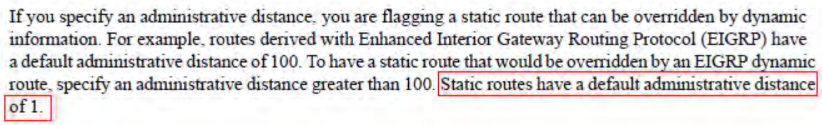
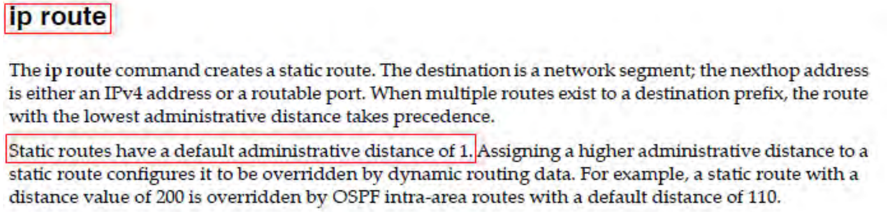
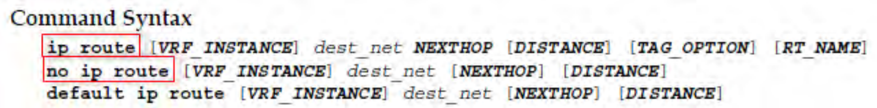
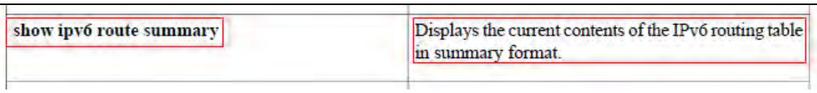
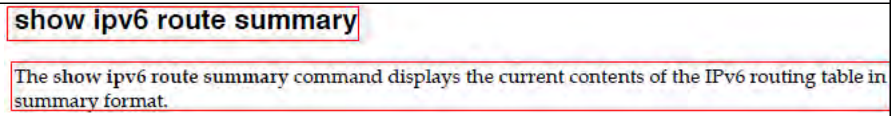
</td>
</tr>
</table>

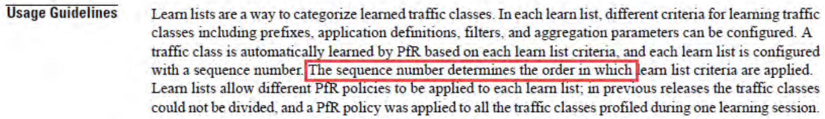
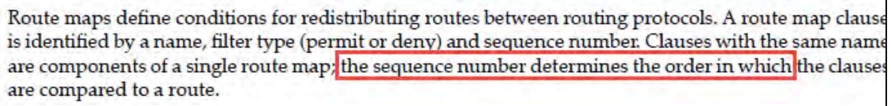
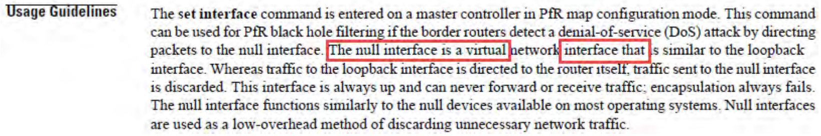
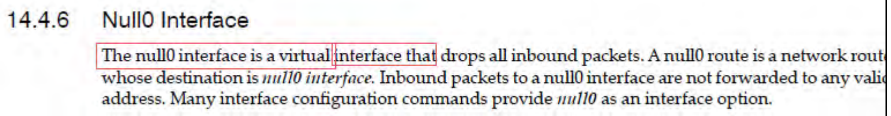
Copyright Registration Information	Cisco	Arista
Cisco IOS 15.4 Effective date of registration: 11/26/2014	 The **show ip bgp summary** command is used to display BGP path, prefix, and attribute information for all connections to BGP neighbors. Cisco IOS IP Routing: BGP Command Reference (2013), at 819.	 **show ip bgp summary**  The **show ip bgp summary** command displays BGP path, prefix, and attribute information for all BGP neighbors. Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1641. *See also* Arista User Manual v. 4.12.3 (7/17/13), at 1407; Arista User Manual, v. 4.11.1 (1/11/13), at 1153; Arista User Manual v. 4.10.3 (10/22/12), at 964; Arista User Manual v. 4.9.3.2 (5/3/12), at 728; Arista User Manual v. 4.8.2 (11/18/11), at 549; Arista User Manual v. 4.7.3 (7/18/11), at 402.
Cisco IOS 12.4 Effective date of registration: 8/12/2005	 The **show ip bgp summary** command is used to display BGP path, prefix, and attribute information for all connections to BGP neighbors. Cisco IOS IP Routing Protocols Command Reference (July 16, 2005), at 323.	 **show ip bgp summary**  The **show ip bgp summary** command displays BGP path, prefix, and attribute information for all BGP neighbors. Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1641. *See also* Arista User Manual v. 4.12.3 (7/17/13), at 1407; Arista User Manual, v. 4.11.1 (1/11/13), at 1153; Arista User Manual v. 4.10.3 (10/22/12), at 964; Arista User Manual v. 4.9.3.2 (5/3/12), at 728; Arista User Manual v. 4.8.2 (11/18/11), at 549; Arista User Manual v. 4.7.3 (7/18/11), at 402.

Copyright Registration Information	Cisco	Arista
Cisco IOS 15.4 Effective date of registration: 11/26/2014	 Up/Down — The length of time that the BGP session has been in the Established state, or the current status if not in the Established state. Cisco IOS IP Routing: BGP Command Reference (2013), at 821.  State/PfxRcd — Current state of the BGP session, and the number of prefixes that have been received from a neighbor or peer group. When the maximum number (as set by the **neighbor maximum-prefix** command) is reached, the string "PfxRcd" appears in the entry, the neighbor is shut down, and the connection is set to Idle. An (Admin) entry with Idle status indicates that the connection has been shut down using the **neighbor shutdown** command. Cisco IOS IP Routing: BGP Command Reference (2013), at 822.	 **Neighbor Table Columns** • (First) Neighbor: IP address of the neighbor. • (Second) V: BGP version number spoken to the neighbor • (Third) AS: Neighbor's Autonomous system number. • (Fourth) MsgRcvd: Number of messages received from the neighbor. • (Fifth) MsgSent: Number of messages sent to the neighbor. • (Sixth) InQ: Number of messages queued to be processed from the neighbor. • (Seventh) OutQ: Number of messages queued to be sent to the neighbor. • (Eighth) Up/Down: Period the BGP session has been in Established state or its current status. • (Ninth) State:State of the BGP session and the number of routes received from a neighbor. After the maximum number of routes are received (maximum paths (BGP)), the field displays PfxRcd, the neighbor is shut down, and the connection is set to Idle. Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1641. *See also* Arista User Manual v. 4.12.3 (7/17/13), at 1407; Arista User Manual, v. 4.11.1 (1/11/13), at 1153; Arista User Manual v. 4.10.3 (10/22/12), at 964; Arista User Manual v. 4.9.3.2 (5/3/12), at 728.
Cisco IOS 12.4 Effective date of registration: 8/12/2005	 Up/Down — The length of time that the BGP session has been in the Established state, or the current state if it is not Established. State/PfxRcd — Current state of the BGP session/the number of prefixes the router has received from a neighbor or peer group. When the maximum number (as set by the **neighbor maximum-prefix** command) is reached, the string "PfxRcd" appears in the entry, the neighbor is shut down, and the connection is Idle. An (Admin) entry with Idle status indicates that the connection has been shut down using the **neighbor shutdown** command. Cisco IOS IP Routing Protocols Command Reference (June 10, 2005), at 318.	 **Neighbor Table Columns** • (First) Neighbor: IP address of the neighbor. • (Second) V: BGP version number spoken to the neighbor • (Third) AS: Neighbor's Autonomous system number. • (Fourth) MsgRcvd: Number of messages received from the neighbor. • (Fifth) MsgSent: Number of messages sent to the neighbor. • (Sixth) InQ: Number of messages queued to be processed from the neighbor. • (Seventh) OutQ: Number of messages queued to be sent to the neighbor. • (Eighth) Up/Down: Period the BGP session has been in Established state or its current status. • (Ninth) State:State of the BGP session and the number of routes received from a neighbor. After the maximum number of routes are received (maximum paths (BGP)), the field displays PfxRcd, the neighbor is shut down, and the connection is set to Idle. Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1641. *See also* Arista User Manual v. 4.12.3 (7/17/13), at 1407; Arista User Manual, v. 4.11.1 (1/11/13), at 1153; Arista User Manual v. 4.10.3 (10/22/12), at 964; Arista User Manual v. 4.9.3.2 (5/3/12), at 728.

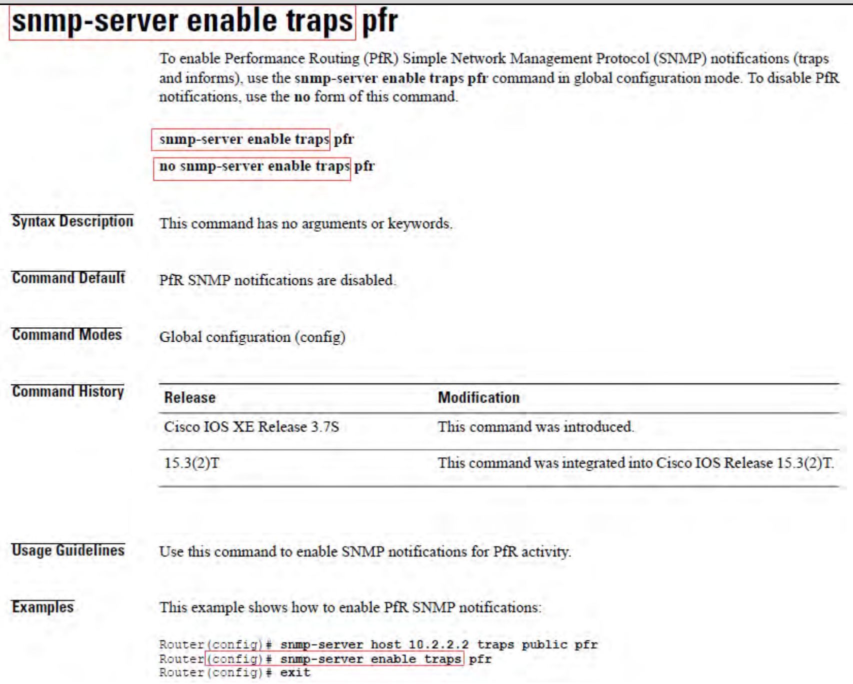
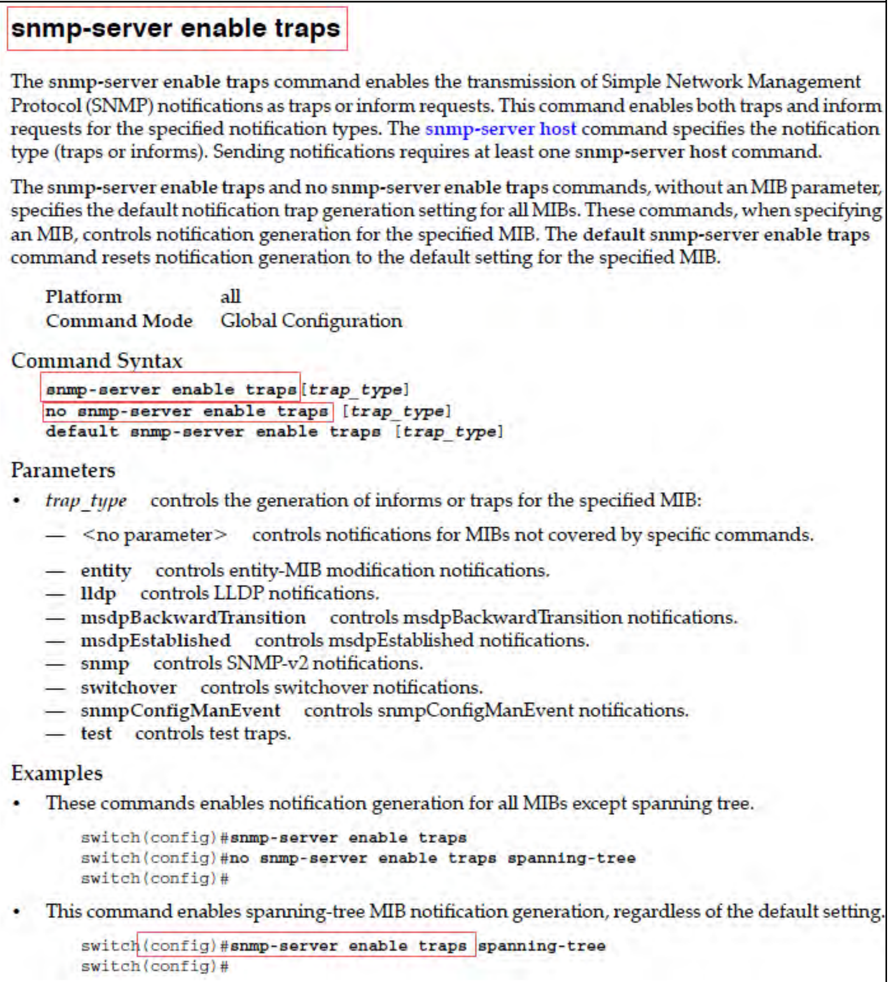
Copyright Registration Information	Cisco	Arista

Cisco IOS 15.4
 	
Effective date of registration: 11/26/2014
	
	bfd
	To set the baseline Bidirectional Forwarding Detection (BFD) session parameters on an interface, use the **bfd** command in interface configuration mode. To remove the baseline BFD session parameters, use the **no** form of this command.
	bfd interval *milliseconds* **min_rx** *milliseconds* **multiplier** *multiplier-value*
	no bfd interval *milliseconds* **min_rx** *milliseconds* **multiplier** *multiplier-value*
	Syntax Description
	interval *milliseconds* — Specifies the rate, in milliseconds, at which BFD control packets will be sent to BFD peers. The valid range for the *milliseconds* argument is from 50 to 999.
	min_rx *milliseconds* — Specifies the rate, in milliseconds, at which BFD control packets will be expected to be received from BFD peers. The valid range for the *milliseconds* argument is from 50 to 999.
	multiplier *multiplier-value* — Specifies the number of consecutive BFD control packets that must be missed from a BFD peer before BFD declares that the peer is unavailable and the Layer 3 BFD peer is informed of the failure. The valid range for the *multiplier-value*argument is from 3 to 50.
	
	Cisco IOS IP Routing: Protocol-Independent Command Reference (2013), at 9
		
		bfd
		The bfd command configures BFD parameters for the configuration mode interface. All BFD sessions that pass through this interface will use these parameters. If custom parameters are not configured, the interface will use default values for BFD sessions passing through it.
		For a BFD session to be established, BFD must be enabled for any routing protocol using BFD for failure detection.
		The **no bfd** and **default bfd** commands return the BFD parameters on the configuration mode interface to default values by removing the corresponding **bfd** command from ***running-config***.
		Platform all
		Command Mode Interface-Ethernet Configuration
		Interface-Loopback Configuration
		Interface-Management Configuration
		Interface-Port-channel Configuration
		Interface-VLAN Configuration
		Command Syntax
		`bfd interval transmit_rate min_rx receive_minimum multiplier factor`
		`no bfd`
		`default bfd`
		Parameters
		• *transmit_rate* specifies the rate in milliseconds at which BFD control packets will be sent to BFD peers. Values range from 50 to 60000; the default value is 300.
		• *receive_minimum* specifies the rate in milliseconds at which BFD control packets will be expected from BFD peers. Values range from 50 to 60000.
		• *factor* specifies the number of consecutive missed BFD control packets from a BFD peer that will designate the peer as unavailable and indicate failure to the Layer 3 BFD peer. Values range from 3 to 50.
		
		Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1741.
		
		See also Arista User Manual v. 4.12.3 (7/17/13), at 1471.

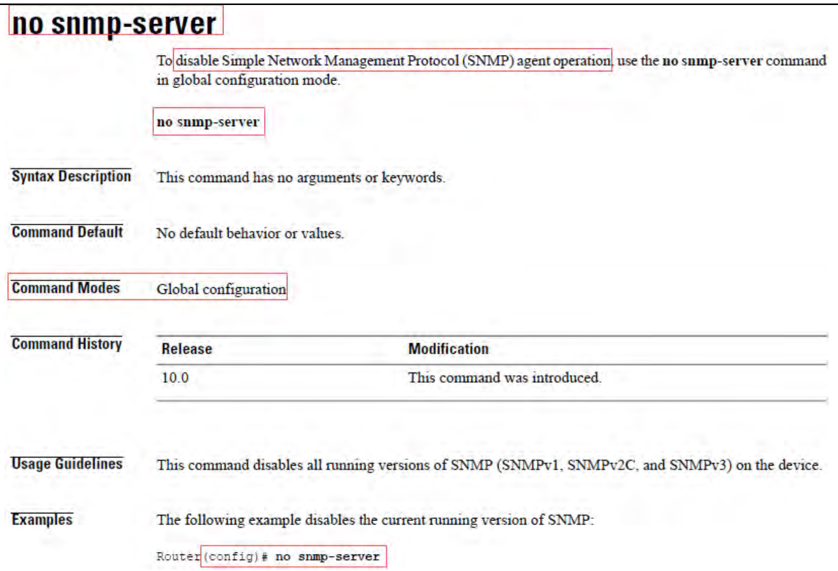
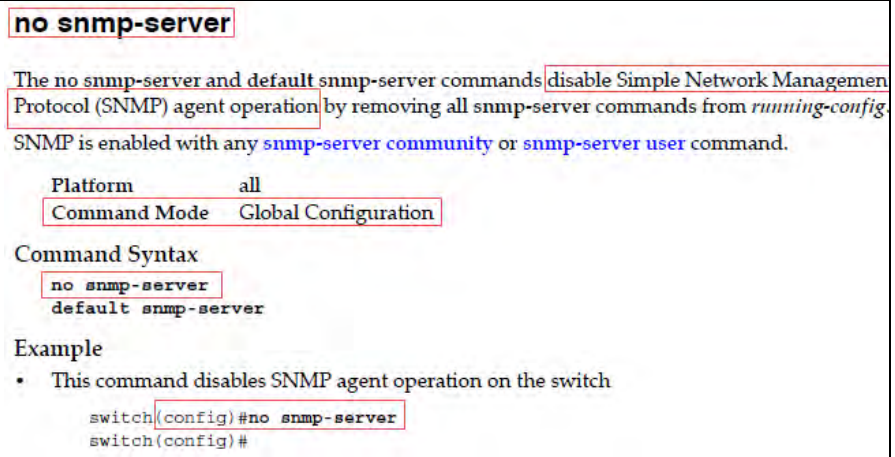
Copyright Registration Information	Cisco	Arista
Cisco IOS 15.4 Effective date of registration: 11/26/2014	 **ip route** To establish static routes, use the**iproute** command in global configuration mode. Toremove static routes, use the **no**form of this command. **ip route** [**vrf** *vrf-name*] *prefix mask* {*ip-address*| *interface-type interface-number* [*ip-address*]} [**dhcp**] [**global**] [*distance*] [**multicast**] [**name** *next-hop-name*] [**permanent**| **track** *number*] [**tag** *tag*] **no ip route** [**vrf** *vrf-name*] *prefix mask* {*ip-address*| *interface-type interface-number* [*ip-address*]} [**dhcp**] [**global**] [*distance*] **multicast** [**name** *next-hop-name*] [**permanent**| **track** *number*] [**tag** *tag*] Cisco IOS IP Routing: Protocol-Independent Command Reference (2013), at 62  If you specify an administrative distance, you are flagging a static route that can be overridden by dynamic information. For example, routes derived with Enhanced Interior Gateway Routing Protocol (EIGRP) have a default administrative distance of 100. To have a static route that would be overridden by an EIGRP dynamic route, specify an administrative distance greater than 100. Static routes have a default administrative distance of 1. Cisco IOS IP Routing: Protocol-Independent Command Reference (2013), at 63	 **ip route** The **ip route** command creates a static route. The destination is a network segment; the nexthop address is either an IPv4 address or a routable port. When multiple routes exist to a destination prefix, the route with the lowest administrative distance takes precedence. Static routes have a default administrative distance of 1. Assigning a higher administrative distance to a static route configures it to be overridden by dynamic routing data. For example, a static route with a distance value of 200 is overridden by OSPF intra-area routes with a default distance of 110. . . .  Command Syntax **ip route** [*VRF_INSTANCE*] *dest_net* *NEXTHOP* [*DISTANCE*] [*TAG_OPTION*] [*RT_NAME*] **no ip route** [*VRF_INSTANCE*] *dest_net* [*NEXTHOP*] [*DISTANCE*] **default ip route** [*VRF_INSTANCE*] *dest_net* [*NEXTHOP*] [*DISTANCE*] Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1287. *See also* Arista User Manual v. 4.12.3 (7/17/13), at 1082; Arista User Manual, v. 4.11.1 (1/11/13), at 860; Arista User Manual v. 4.10.3 (10/22/12), at 683.
Cisco IOS 15.4 Effective date of registration: 11/26/2014	 **show ipv6 route summary** — Displays the current contents of the IPv6 routing table in summary format. Cisco IOS IP Routing: Protocol-Independent Command Reference (2013), at 284	 **show ipv6 route summary** The **show ipv6 route summary** command displays the current contents of the IPv6 routing table in summary format. Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1337. *See also* Arista User Manual v. 4.12.3 (7/17/13), at 1165.

Copyright Registration Information	Cisco	Arista
Cisco IOS 15.4 Effective date of registration: 11/26/2014	 **Usage Guidelines** Learn lists are a way to categorize learned traffic classes. In each learn list, different criteria for learning traffic classes including prefixes, application definitions, filters, and aggregation parameters can be configured. A traffic class is automatically learned by PfR based on each learn list criteria, and each learn list is configured with a sequence number. The sequence number determines the order in which learn list criteria are applied. Learn lists allow different PfR policies to be applied to each learn list; in previous releases the traffic classes could not be divided, and a PfR policy was applied to all the traffic classes profiled during one learning session. Cisco IOS Performance Routing Command Reference (2010), at 131.	 Route maps define conditions for redistributing routes between routing protocols. A route map clause is identified by a name, filter type (permit or deny) and sequence number. Clauses with the same name are components of a single route map; the sequence number determines the order in which the clauses are compared to a route. Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 894. *See also* Arista User Manual v. 4.12.3 (7/17/13), at 773; Arista User Manual, v. 4.11.1 (1/11/13), at 602; Arista User Manual v. 4.10.3 (10/22/12), at 516; Arista User Manual v. 4.9.3.2 (5/3/12), at 439; Arista User Manual v. 4.8.2 (11/18/11), at 316.
Cisco IOS 15.4 Effective date of registration: 11/26/2014	 **Usage Guidelines** The **set interface** command is entered on a master controller in PfR map configuration mode. This command can be used for PfR black hole filtering if the border routers detect a denial-of-service (DoS) attack by directing packets to the null interface. The null interface is a virtual network interface that is similar to the loopback interface. Whereas traffic to the loopback interface is directed to the router itself, traffic sent to the null interface is discarded. This interface is always up and can never forward or receive traffic; encapsulation always fails. The null interface functions similarly to the null devices available on most operating systems. Null interfaces are used as a low-overhead method of discarding unnecessary network traffic. Cisco IOS Performance Routing Command Reference (2010), at 226.	 14.4.6 Null0 Interface The null0 interface is a virtual interface that drops all inbound packets. A null0 route is a network rout whose destination is *null0 interface*. Inbound packets to a null0 interface are not forwarded to any vali address. Many interface configuration commands provide *null0* as an interface option. Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 633. *See also* Arista User Manual v. 4.12.3 (7/17/13), at 502; Arista User Manual, v. 4.11.1 (1/11/13), at 397; Arista User Manual v. 4.10.3 (10/22/12), at 329.

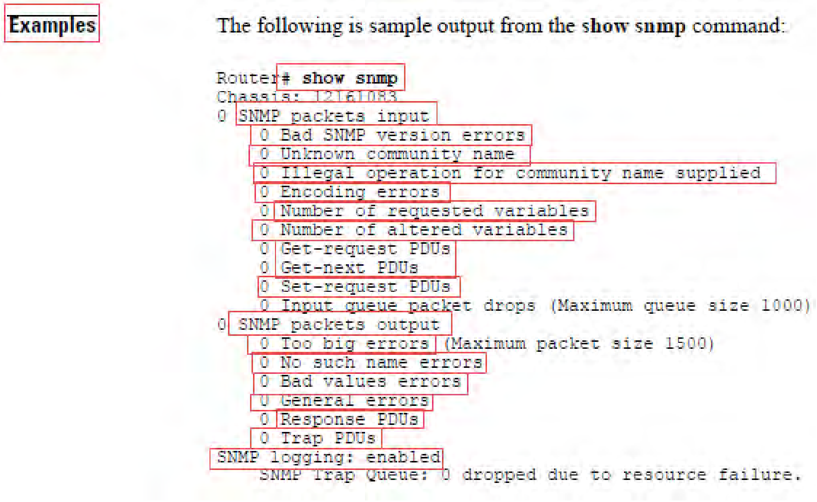
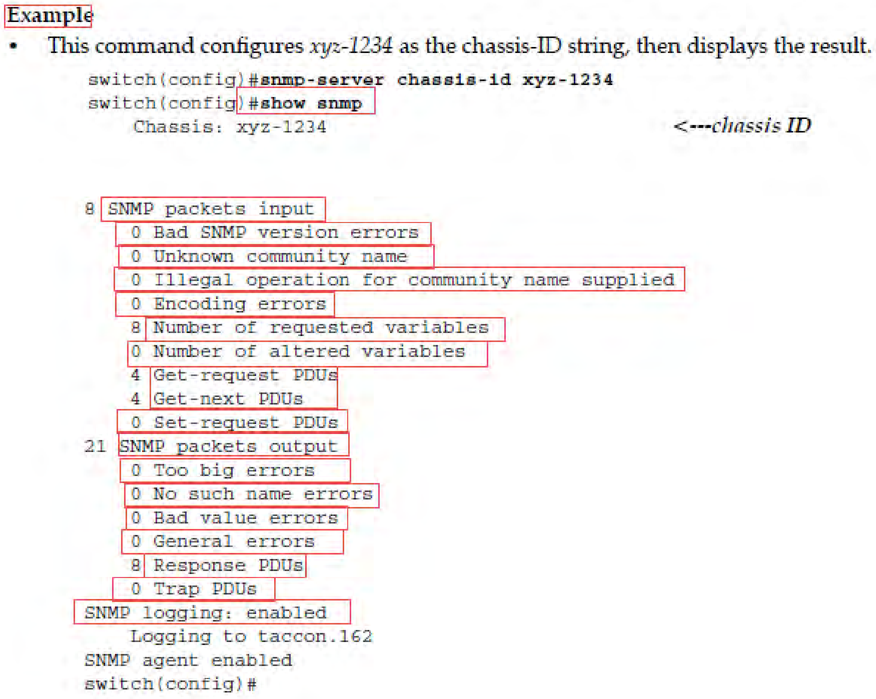
Copyright Registration Information	Cisco	Arista

Cisco IOS 15.4
Effective date of registration: 11/26/2014
	
	snmp-server enable traps pfr
	To enable Performance Routing (PfR) Simple Network Management Protocol (SNMP) notifications (traps and informs), use the **snmp-server enable traps pfr** command in global configuration mode. To disable PfR notifications, use the **no** form of this command.
	snmp-server enable traps pfr
	no snmp-server enable traps pfr
	Syntax Description This command has no arguments or keywords.
	Command Default PfR SNMP notifications are disabled.
	Command Modes Global configuration (config)
	Command History
	Release — **Modification**
	Cisco IOS XE Release 3.7S — This command was introduced.
	15.3(2)T — This command was integrated into Cisco IOS Release 15.3(2)T.
	Usage Guidelines Use this command to enable SNMP notifications for PfR activity.
	Examples This example shows how to enable PfR SNMP notifications:
	`Router(config)# snmp-server host 10.2.2.2 traps public pfr`
	`Router(config)# snmp-server enable traps pfr`
	`Router(config)# exit`
	Cisco IOS Performance Routing Command Reference (2010), at 372.
		
		snmp-server enable traps
		The **snmp-server enable traps** command enables the transmission of Simple Network Management Protocol (SNMP) notifications as traps or inform requests. This command enables both traps and inform requests for the specified notification types. The snmp-server host command specifies the notification type (traps or informs). Sending notifications requires at least one snmp-server host command.
		The **snmp-server enable traps** and **no snmp-server enable traps** commands, without an MIB parameter, specifies the default notification trap generation setting for all MIBs. These commands, when specifying an MIB, controls notification generation for the specified MIB. The **default snmp-server enable traps** command resets notification generation to the default setting for the specified MIB.
		Platform all
		Command Mode Global Configuration
		Command Syntax
		`snmp-server enable traps[trap_type]`
		`no snmp-server enable traps [trap_type]`
		`default snmp-server enable traps [trap_type]`
		Parameters
		• *trap_type* controls the generation of informs or traps for the specified MIB:
		— <no parameter> controls notifications for MIBs not covered by specific commands.
		— **entity** controls entity-MIB modification notifications.
		— **lldp** controls LLDP notifications.
		— **msdpBackwardTransition** controls msdpBackwardTransition notifications.
		— **msdpEstablished** controls msdpEstablished notifications.
		— **snmp** controls SNMP-v2 notifications.
		— **switchover** controls switchover notifications.
		— **snmpConfigManEvent** controls snmpConfigManEvent notifications.
		— **test** controls test traps.
		Examples
		• These commands enables notification generation for all MIBs except spanning tree.
		`switch(config)#snmp-server enable traps`
		`switch(config)#no snmp-server enable traps spanning-tree`
		`switch(config)#`
		• This command enables spanning-tree MIB notification generation, regardless of the default setting.
		`switch(config)#snmp-server enable traps spanning-tree`
		`switch(config)#`
		Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1990.
		See also Arista User Manual v. 4.12.3 (7/17/13), at 1680; Arista User Manual, v. 4.11.1 (1/11/13), at 1365; Arista User Manual v. 4.10.3 (10/22/12), at 1132; Arista User Manual v. 4.9.3.2 (5/3/12), at 888; Arista

Copyright Registration Information	Cisco	Arista
		User Manual v. 4.8.2 (11/18/11), at 696; Arista User Manual v. 4.7.3 (7/18/11), at 552.

Cisco IOS 15.4
Effective date of registration: 11/26/2014
	
	no snmp-server
	To disable Simple Network Management Protocol (SNMP) agent operation, use the **no snmp-server** command in global configuration mode.
	`no snmp-server`
	Syntax Description This command has no arguments or keywords.
	Command Default No default behavior or values.
	Command Modes Global configuration
	Command History **Release** / **Modification**: 10.0 / This command was introduced.
	Usage Guidelines This command disables all running versions of SNMP (SNMPv1, SNMPv2C, and SNMPv3) on the device.
	Examples The following example disables the current running version of SNMP:
	`Router(config)# no snmp-server`
	Cisco IOS SNMP Support Command Reference (2013), at 52.
		
		no snmp-server
		The no snmp-server and default snmp-server commands disable Simple Network Managemen Protocol (SNMP) agent operation by removing all snmp-server commands from *running-config*. SNMP is enabled with any snmp-server community or snmp-server user command.
		Platform all
		Command Mode Global Configuration
		Command Syntax
		`no snmp-server`
		`default snmp-server`
		Example
		• This command disables SNMP agent operation on the switch
		`switch(config)#no snmp-server`
		`switch(config)#`
		Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1973.
		See also Arista User Manual v. 4.12.3 (7/17/13), at 1663; Arista User Manual, v. 4.11.1 (1/11/13), at 1350; Arista User Manual v. 4.10.3 (10/22/12), at 1117; Arista User Manual v. 4.9.3.2 (5/3/12), at 873; Arista User Manual v. 4.8.2 (11/18/11), at 681; Arista User Manual v. 4.7.3 (7/18/11), at 537.

Copyright Registration Information	Cisco	Arista

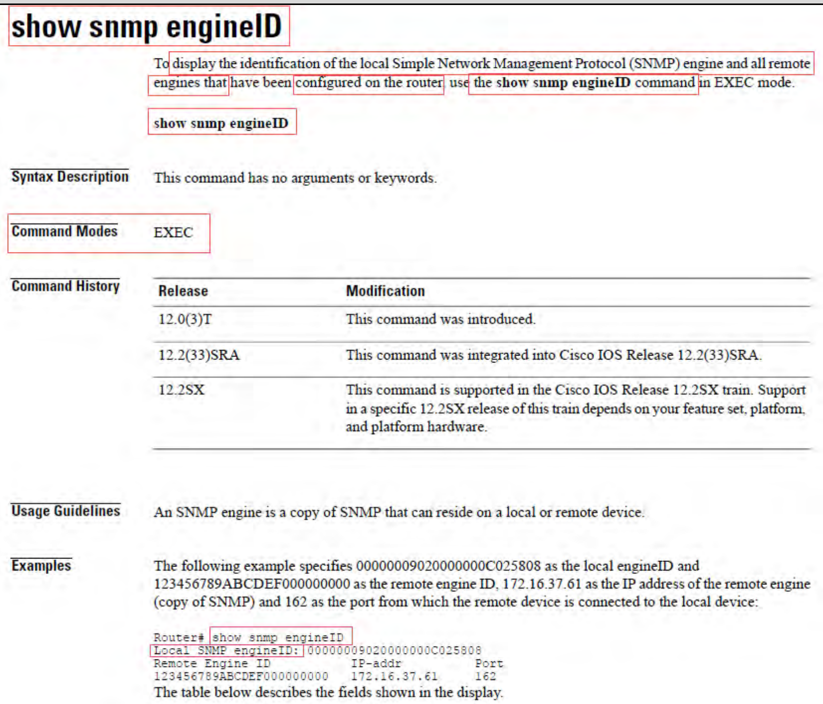
Cisco IOS 15.4
 	
Effective date of registration: 11/26/2014
	
	Examples
	The following is sample output from the **show snmp** command:
	`Router# show snmp`
	`Chassis: 12161083`
	`0 SNMP packets input`
	`    0 Bad SNMP version errors`
	`    0 Unknown community name`
	`    0 Illegal operation for community name supplied`
	`    0 Encoding errors`
	`    0 Number of requested variables`
	`    0 Number of altered variables`
	`    0 Get-request PDUs`
	`    0 Get-next PDUs`
	`    0 Set-request PDUs`
	`    0 Input queue packet drops (Maximum queue size 1000)`
	`0 SNMP packets output`
	`    0 Too big errors (Maximum packet size 1500)`
	`    0 No such name errors`
	`    0 Bad values errors`
	`    0 General errors`
	`    0 Response PDUs`
	`    0 Trap PDUs`
	`SNMP logging: enabled`
	`    SNMP Trap Queue: 0 dropped due to resource failure.`
	
	Cisco IOS SNMP Support Command Reference (2013), at 83.
		
		Example
		- This command configures *xyz-1234* as the chassis-ID string, then displays the result.
		`switch(config)#snmp-server chassis-id xyz-1234`
		`switch(config)#show snmp`
		`    Chassis: xyz-1234` *<---chassis ID*
		`8 SNMP packets input`
		`    0 Bad SNMP version errors`
		`    0 Unknown community name`
		`    0 Illegal operation for community name supplied`
		`    0 Encoding errors`
		`    8 Number of requested variables`
		`    0 Number of altered variables`
		`    4 Get-request PDUs`
		`    4 Get-next PDUs`
		`    0 Set-request PDUs`
		`21 SNMP packets output`
		`    0 Too big errors`
		`    0 No such name errors`
		`    0 Bad value errors`
		`    0 General errors`
		`    8 Response PDUs`
		`    0 Trap PDUs`
		`SNMP logging: enabled`
		`    Logging to taccon.162`
		`SNMP agent enabled`
		`switch(config)#`
		
		Arista User Manual v. 4.14.3F (Rev. 2) (October 2, 2014), at 1967-68.
		
		See also Arista User Manual v. 4.13.6F (4/14/2014), at 1896; Arista User Manual v. 4.12.3 (7/17/13), at 1658; Arista User Manual, v. 4.11.1 (1/11/13), at 1344-45; Arista User Manual v. 4.10.3 (10/22/12), at 1111; Arista User Manual v. 4.9.3.2 (5/3/12), at 867; Arista User Manual v. 4.8.2 (11/18/11), at 678; Arista User Manual v. 4.7.3 (7/18/11), at 534.

<table>
<tr>
<th>Copyright Registration Information</th>
<th>Cisco</th>
<th>Arista</th>
</tr>
<tr>
<td>

Cisco IOS 15.4

Effective date of registration: 11/26/2014

</td>
<td>



show snmp engineID

To display the identification of the local Simple Network Management Protocol (SNMP) engine and all remote engines that have been configured on the router, use the **show snmp engineID** command in EXEC mode.

show snmp engineID

Syntax Description This command has no arguments or keywords.

Command Modes EXEC

Command History

Release	Modification
12.0(3)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines An SNMP engine is a copy of SNMP that can reside on a local or remote device.

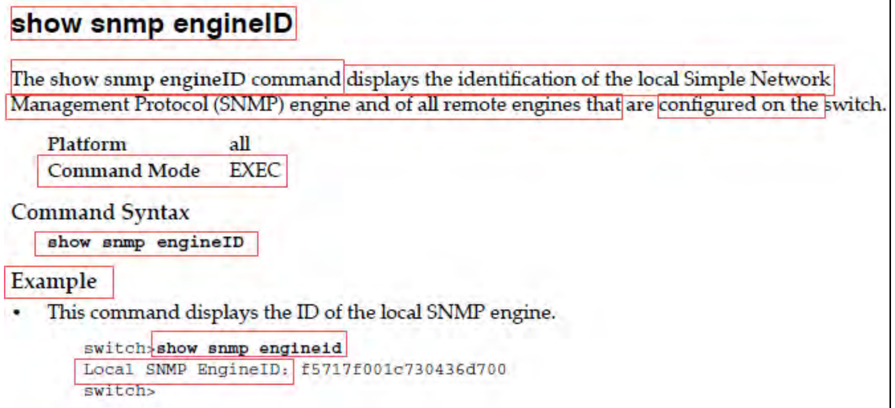
Examples The following example specifies 00000009020000000C025808 as the local engineID and 123456789ABCDEF000000000 as the remote engine ID, 172.16.37.61 as the IP address of the remote engine (copy of SNMP) and 162 as the port from which the remote device is connected to the local device:

```
Router# show snmp engineID
Local SNMP engineID: 00000009020000000C025808
Remote Engine ID          IP-addr          Port
123456789ABCDEF000000000  172.16.37.61     162
```

The table below describes the fields shown in the display.

Cisco IOS SNMP Support Command Reference (2013), at 91.

</td>
<td>



show snmp engineID

The show snmp engineID command displays the identification of the local Simple Network Management Protocol (SNMP) engine and of all remote engines that are configured on the switch.

Platform	all
Command Mode	EXEC

Command Syntax

```
show snmp engineID
```

Example

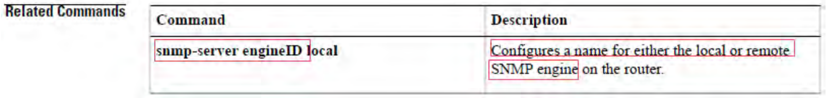
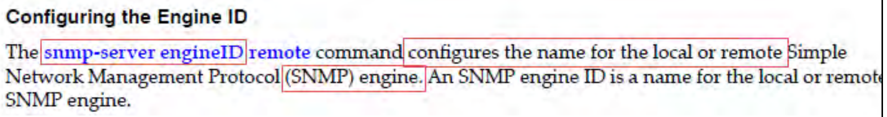
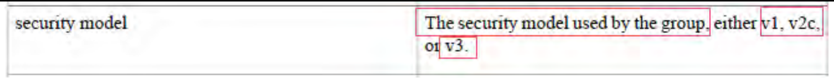
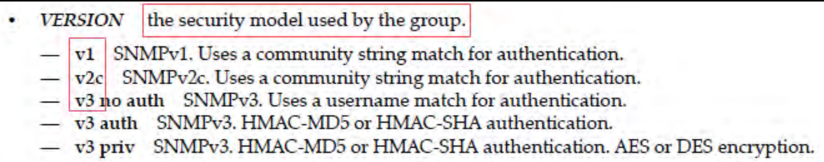
- This command displays the ID of the local SNMP engine.

```
switch>show snmp engineid
Local SNMP EngineID: f5717f001c730436d700
switch>
```

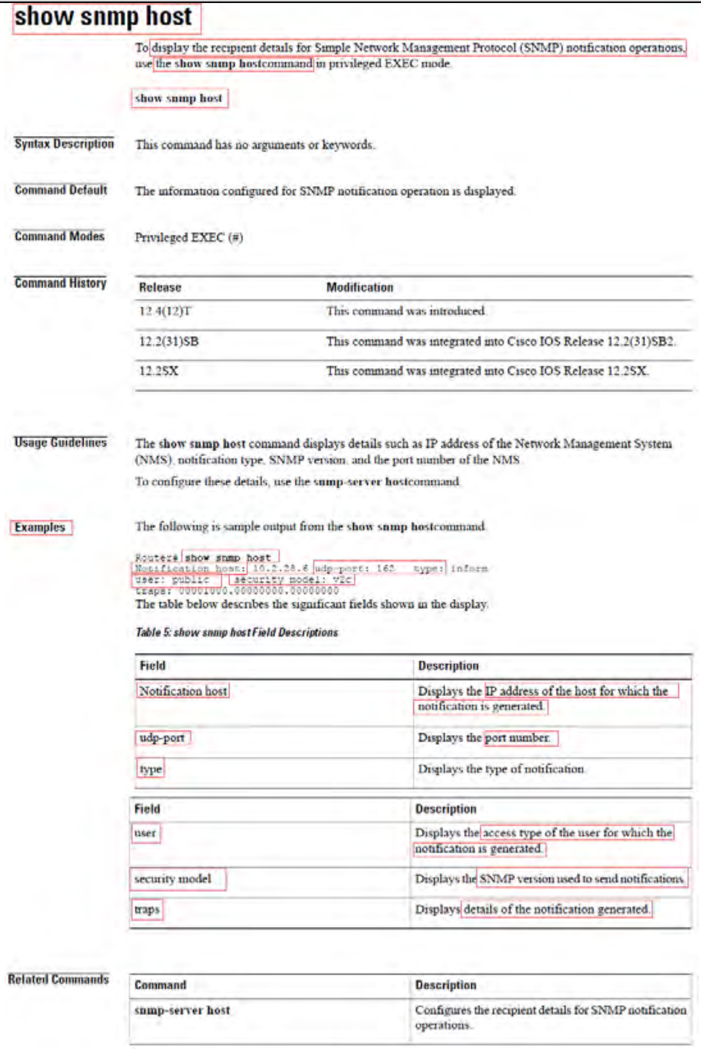
Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1978.

See also Arista User Manual v. 4.12.3 (7/17/13), at 1668; Arista User Manual, v. 4.11.1 (1/11/13), at 1355; Arista User Manual v. 4.10.3 (10/22/12), at 1122; Arista User Manual v. 4.9.3.2 (5/3/12), at 878; Arista User Manual v. 4.8.2 (11/18/11), at 686; Arista User Manual v. 4.7.3 (7/18/11), at 542.

</td>
</tr>
</table>

Copyright Registration Information	Cisco	Arista
Cisco IOS 15.4 Effective date of registration: 11/26/2014	 Related Commands Command — Description snmp-server engineID local — Configures a name for either the local or remote SNMP engine on the router. Cisco IOS SNMP Support Command Reference (2013), at 92.	 Configuring the Engine ID The snmp-server engineID remote command configures the name for the local or remote Simple Network Management Protocol (SNMP) engine. An SNMP engine ID is a name for the local or remote SNMP engine. Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1966. *See also* Arista User Manual v. 4.13.6F (4/14/2014), at 1894; Arista User Manual v. 4.12.3 (7/17/13), at 1656; Arista User Manual, v. 4.11.1 (1/11/13), at 1343; Arista User Manual v. 4.10.3 (10/22/12), at 1109; Arista User Manual v. 4.9.3.2 (5/3/12), at 865; Arista User Manual v. 4.8.2 (11/18/11), at 676; Arista User Manual v. 4.7.3 (7/18/11), at 432.
Cisco IOS 15.4 Effective date of registration: 11/26/2014	 security model — The security model used by the group, either v1, v2c, or v3. Cisco IOS SNMP Support Command Reference (2013), at 92.	 • *VERSION* the security model used by the group. — v1 SNMPv1. Uses a community string match for authentication. — v2c SNMPv2c. Uses a community string match for authentication. — v3 no auth SNMPv3. Uses a username match for authentication. — v3 auth SNMPv3. HMAC-MD5 or HMAC-SHA authentication. — v3 priv SNMPv3. HMAC-MD5 or HMAC-SHA authentication. AES or DES encryption. Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1994. *See also* Arista User Manual v. 4.12.3 (7/17/13), at 1684; Arista User Manual, v. 4.11.1 (1/11/13), at 1369; Arista User Manual v. 4.10.3 (10/22/12), at 1136; Arista User Manual v. 4.9.3.2 (5/3/12), at 892; Arista User Manual v. 4.8.2 (11/18/11), at 699; Arista User Manual v. 4.7.3 (7/18/11), at 555.

<table>
<tr><th>Copyright Registration Information</th><th>Cisco</th><th>Arista</th></tr>
<tr>
<td>Cisco IOS 15.4

Effective date of registration: 11/26/2014</td>
<td>
show snmp host

To display the recipient details for Simple Network Management Protocol (SNMP) notification operations, use the <b>show snmp host</b>command in privileged EXEC mode.

<b>show snmp host</b>

Syntax Description — This command has no arguments or keywords.

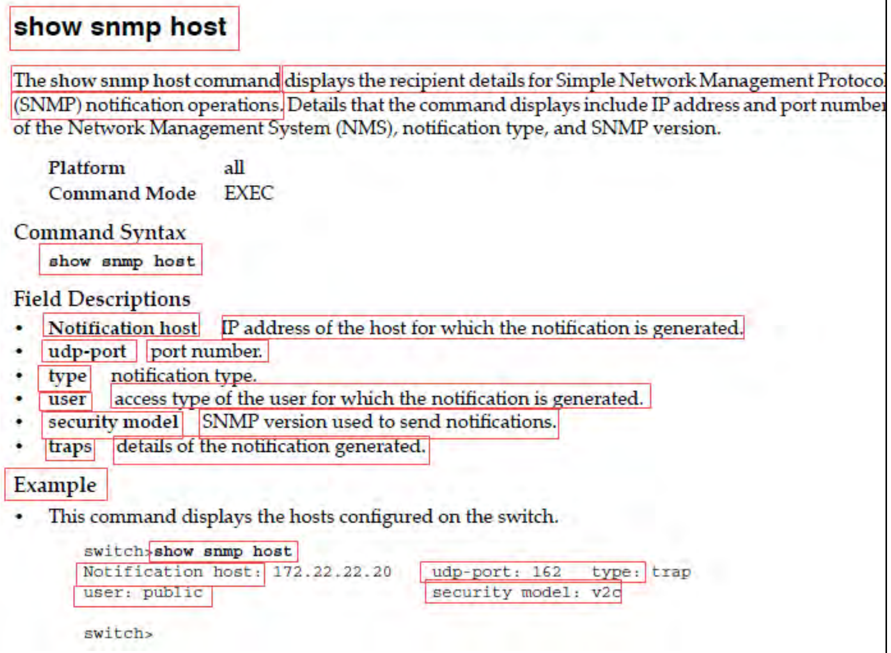
Command Default — The information configured for SNMP notification operation is displayed.

Command Modes — Privileged EXEC (#)

Command History
<table><tr><th>Release</th><th>Modification</th></tr><tr><td>12.4(12)T</td><td>This command was introduced.</td></tr><tr><td>12.2(31)SB</td><td>This command was integrated into Cisco IOS Release 12.2(31)SB2.</td></tr><tr><td>12.2SX</td><td>This command was integrated into Cisco IOS Release 12.2SX.</td></tr></table>
Usage Guidelines — The <b>show snmp host</b> command displays details such as IP address of the Network Management System (NMS), notification type, SNMP version, and the port number of the NMS.
To configure these details, use the <b>snmp-server host</b>command.

Examples — The following is sample output from the <b>show snmp host</b>command.

Router# show snmp host
Notification host: 10.2.28.6 udp-port: 162   type: inform
user: public   security model: v2c
traps: 00001000.00000000.00000000
The table below describes the significant fields shown in the display.

<i>Table 5: show snmp host Field Descriptions</i>
<table><tr><th>Field</th><th>Description</th></tr><tr><td>Notification host</td><td>Displays the IP address of the host for which the notification is generated.</td></tr><tr><td>udp-port</td><td>Displays the port number.</td></tr><tr><td>type</td><td>Displays the type of notification.</td></tr></table><table><tr><th>Field</th><th>Description</th></tr><tr><td>user</td><td>Displays the access type of the user for which the notification is generated.</td></tr><tr><td>security model</td><td>Displays the SNMP version used to send notifications.</td></tr><tr><td>traps</td><td>Displays details of the notification generated.</td></tr></table>
Related Commands
<table><tr><th>Command</th><th>Description</th></tr><tr><td><b>snmp-server host</b></td><td>Configures the recipient details for SNMP notification operations.</td></tr></table>
Cisco IOS SNMP Support Command Reference (2013), at 95-96.</td>
<td>
show snmp host

The show snmp host command displays the recipient details for Simple Network Management Protocol (SNMP) notification operations. Details that the command displays include IP address and port number of the Network Management System (NMS), notification type, and SNMP version.

Platform all
Command Mode EXEC

Command Syntax
<b>show snmp host</b>

Field Descriptions
• <b>Notification host</b> IP address of the host for which the notification is generated.
• <b>udp-port</b> port number.
• <b>type</b> notification type.
• <b>user</b> access type of the user for which the notification is generated.
• <b>security model</b> SNMP version used to send notifications.
• <b>traps</b> details of the notification generated.

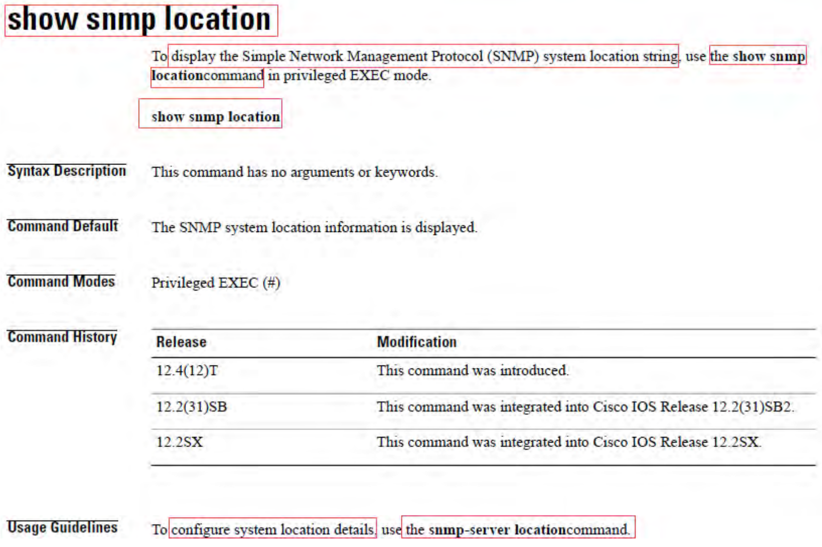
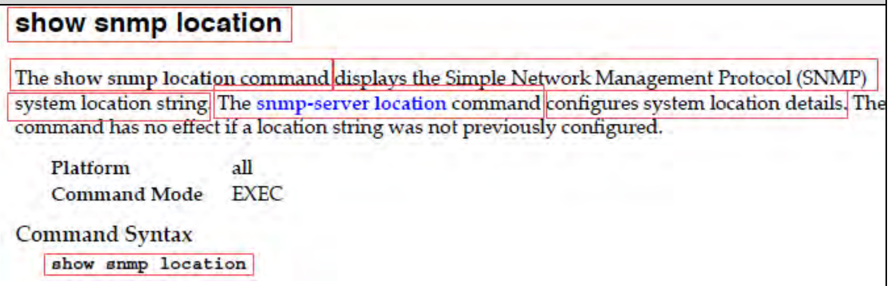
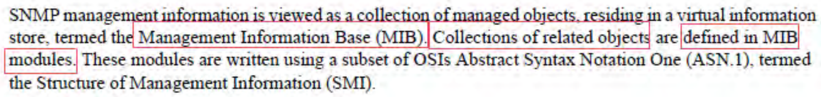
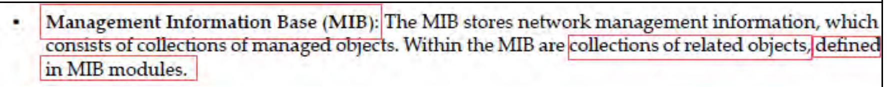
Example
• This command displays the hosts configured on the switch.

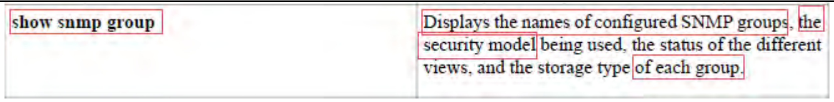
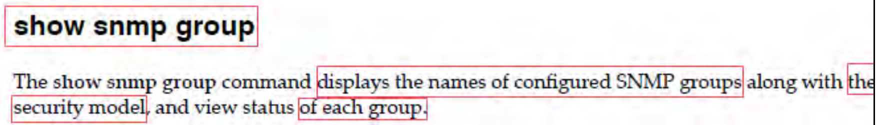
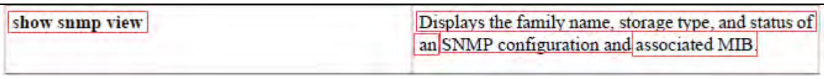
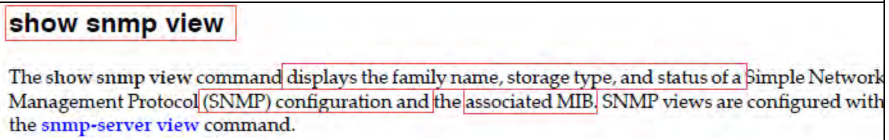
switch>show snmp host
Notification host: 172.22.22.20   udp-port: 162   type: trap
user: public   security model: v2c

switch>

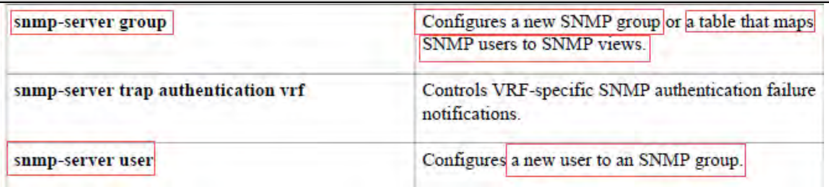
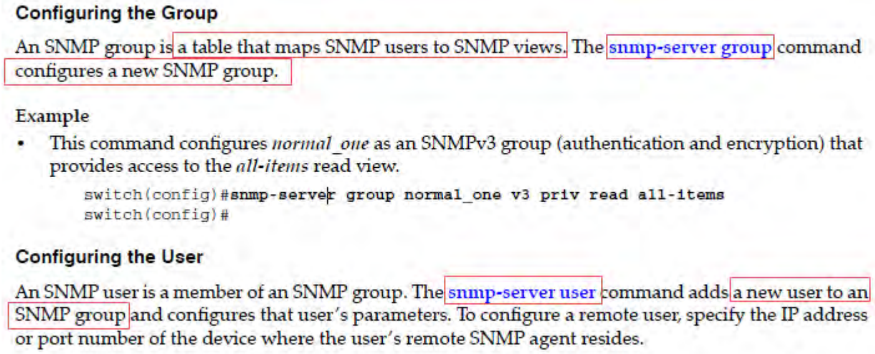
Arista User Manual v.4.14.3F (Rev. 2) (10/2/2014), at 1980.

<i>See also</i> Arista User Manual v. 4.13.6F (4/14/2014), at 1908; Arista User Manual v. 4.12.3 (7/17/13), at 1670; Arista User Manual, v. 4.11.1 (1/11/13), at 1357; Arista User Manual v. 4.10.3 (10/22/12), at 1124; Arista User Manual v. 4.9.3.2 (5/3/12), at 880; Arista User Manual v. 4.8.2 (11/18/11), at 688; Arista User Manual v. 4.7.3 (7/18/11), at 544.</td>
</tr>
</table>

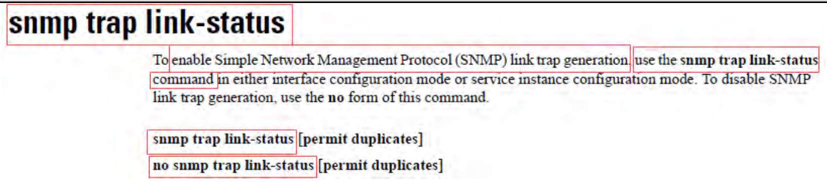
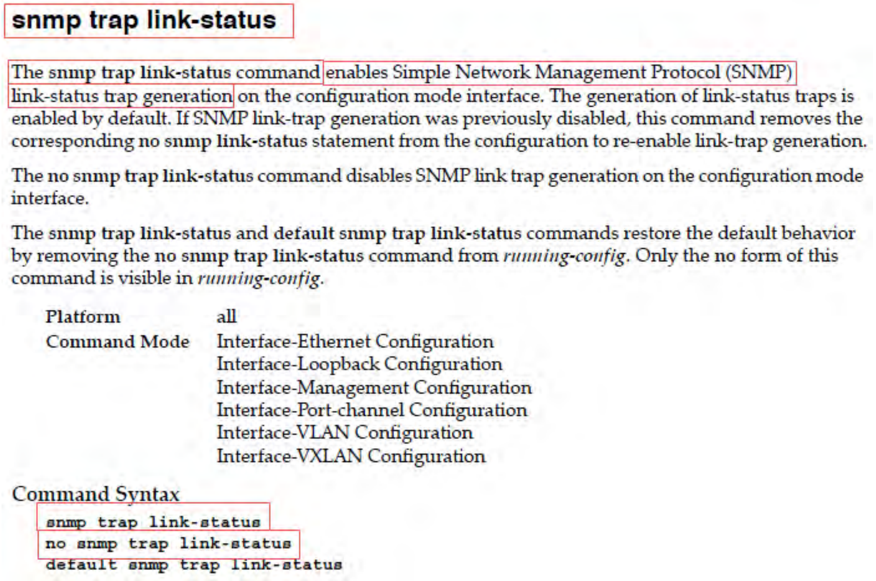
Copyright Registration Information	Cisco	Arista
Cisco IOS 15.4 Effective date of registration: 11/26/2014	 **show snmp location** To display the Simple Network Management Protocol (SNMP) system location string, use the **show snmp location**command in privileged EXEC mode. **show snmp location** **Syntax Description** This command has no arguments or keywords. **Command Default** The SNMP system location information is displayed. **Command Modes** Privileged EXEC (#) **Command History** **Release** — **Modification** 12.4(12)T — This command was introduced. 12.2(31)SB — This command was integrated into Cisco IOS Release 12.2(31)SB2. 12.2SX — This command was integrated into Cisco IOS Release 12.2SX. **Usage Guidelines** To configure system location details, use the **snmp-server location**command. Cisco IOS SNMP Support Command Reference (2013), at 97.	 **show snmp location** The show snmp location command displays the Simple Network Management Protocol (SNMP) system location string The snmp-server location command configures system location details. The command has no effect if a location string was not previously configured. Platform all Command Mode EXEC Command Syntax `show snmp location` Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1980. *See also* Arista User Manual v. 4.12.3 (7/17/13), at 1671; Arista User Manual, v. 4.11.1 (1/11/13), at 1358; Arista User Manual v. 4.10.3 (10/22/12), at 1125; Arista User Manual v. 4.9.3.2 (5/3/12), at 881; Arista User Manual v. 4.8.2 (11/18/11), at 689; Arista User Manual v. 4.7.3 (7/18/11), at 545.
Cisco IOS 15.4 Effective date of registration: 11/26/2014	 SNMP management information is viewed as a collection of managed objects, residing in a virtual information store, termed the Management Information Base (MIB). Collections of related objects are defined in MIB modules. These modules are written using a subset of OSIs Abstract Syntax Notation One (ASN.1), termed the Structure of Management Information (SMI). Cisco IOS SNMP Support Command Reference (2013), at 98..	 • Management Information Base (MIB): The MIB stores network management information, which consists of collections of managed objects. Within the MIB are collections of related objects, defined in MIB modules. Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1961. *See also* Arista User Manual v. 4.12.3 (7/17/13), at 1651; Arista User Manual, v. 4.11.1 (1/11/13), at 1339; Arista User Manual v. 4.10.3 (10/22/12), at 1105; Arista User Manual v. 4.9.3.2 (5/3/12), at 861; Arista User Manual v. 4.8.2 (11/18/11), at 673; Arista User Manual v. 4.7.3 (7/18/11), at 529.

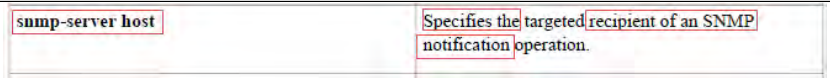
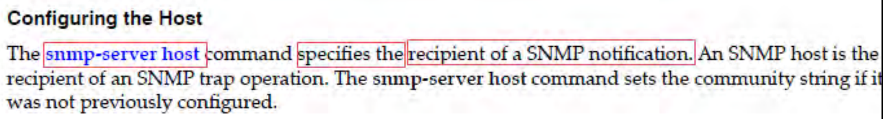
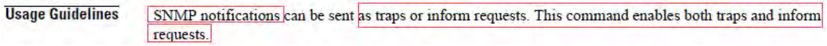
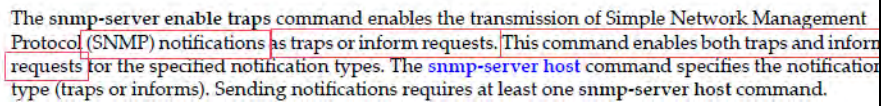
Copyright Registration Information	Cisco	Arista
Cisco IOS 15.4 Effective date of registration: 11/26/2014	 show snmp group Displays the names of configured SNMP groups, the security model being used, the status of the different views, and the storage type of each group. Cisco IOS SNMP Support Command Reference (2013), at 123.	 show snmp group The show snmp group command displays the names of configured SNMP groups along with the security model, and view status of each group. Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1971 *See also* Arista User Manual v. 4.12.3 (7/17/13), at 1669; Arista User Manual, v. 4.11.1 (1/11/13), at 1356; Arista User Manual v. 4.10.3 (10/22/12), at 1123; Arista User Manual v. 4.9.3.2 (5/3/12), at 879; Arista User Manual v. 4.8.2 (11/18/11), at 687; Arista User Manual v. 4.7.3 (7/18/11), at 543.
Cisco IOS 15.4 Effective date of registration: 11/26/2014	 show snmp view Displays the family name, storage type, and status of an SNMP configuration and associated MIB. Cisco IOS SNMP Support Command Reference (2013), at 123.	 show snmp view The show snmp view command displays the family name, storage type, and status of a Simple Network Management Protocol (SNMP) configuration and the associated MIB. SNMP views are configured with the snmp-server view command. Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1986. *See also* Arista User Manual v. 4.13.6F (4/14/2014), at 1914; Arista User Manual v. 4.12.3 (7/17/13), at 1676; Arista User Manual, v. 4.11.1 (1/11/13), at 1361; Arista User Manual v. 4.10.3 (10/22/12), at 1128; Arista User Manual v. 4.9.3.2 (5/3/12), at 884; Arista User Manual v. 4.8.2 (11/18/11), at 692; Arista User Manual v. 4.7.3 (7/18/11), at 548.

Copyright Registration Information	Cisco	Arista

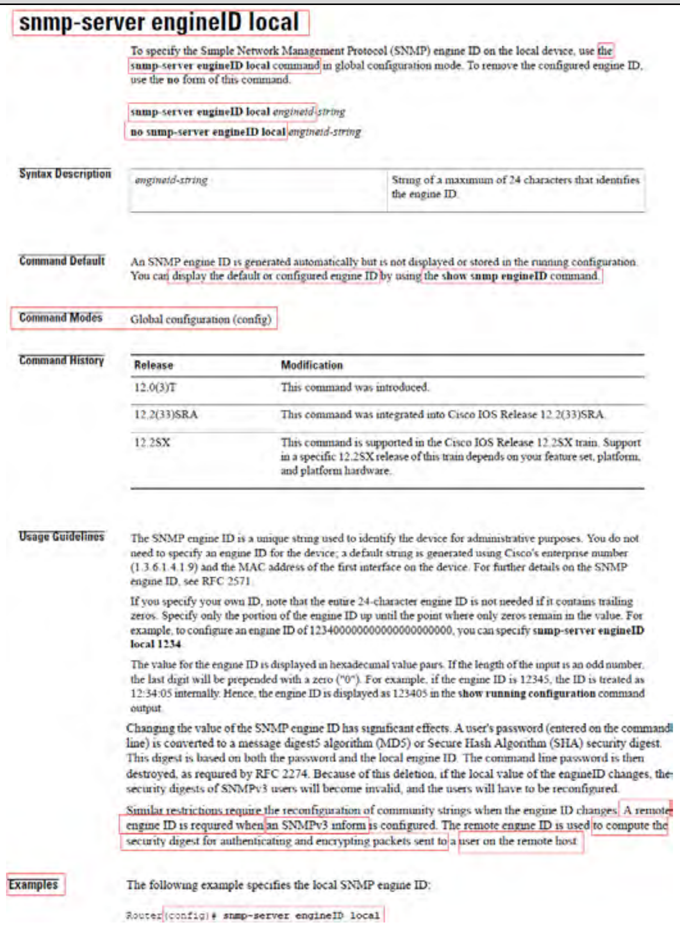
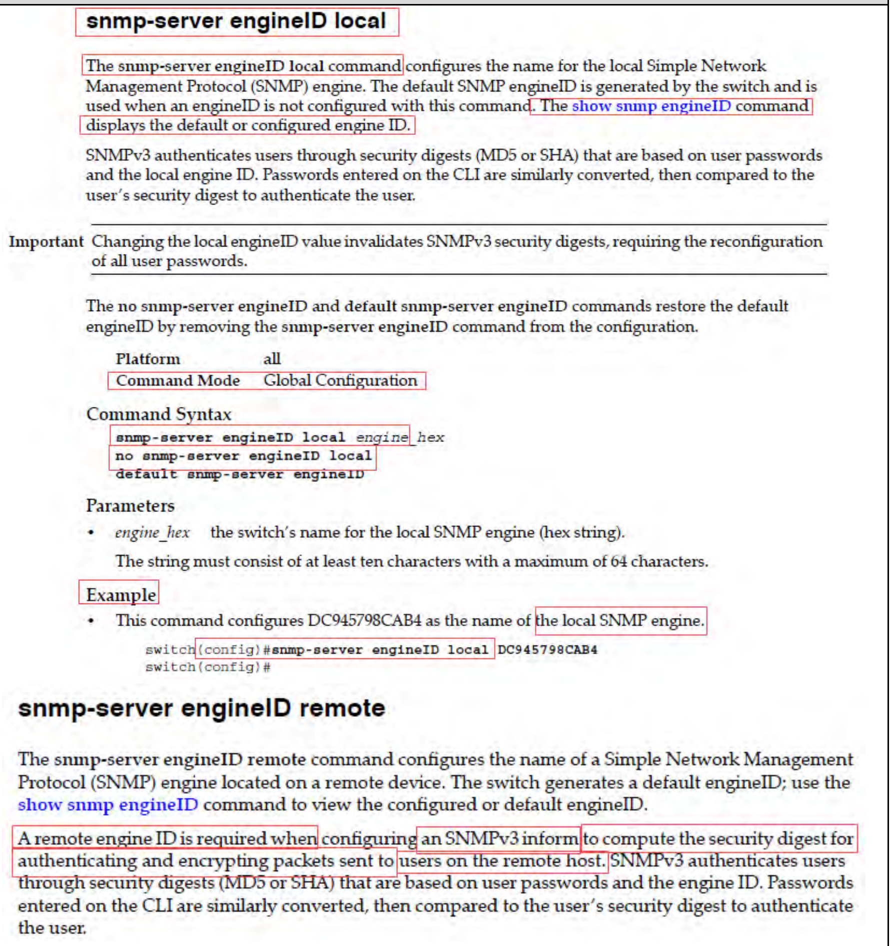
Cisco IOS 15.4
 	
Effective date of registration: 11/26/2014
	
	snmp-server group
	Configures a new SNMP group or a table that maps SNMP users to SNMP views.
	snmp-server trap authentication vrf
	Controls VRF-specific SNMP authentication failure notifications.
	snmp-server user
	Configures a new user to an SNMP group.
	
	Cisco IOS SNMP Support Command Reference (2013), at 130.
		
		Configuring the Group
		An SNMP group is a table that maps SNMP users to SNMP views. The snmp-server group command configures a new SNMP group.
		Example
		• This command configures *normal_one* as an SNMPv3 group (authentication and encryption) that provides access to the *all-items* read view.
		`switch(config)#snmp-server group normal_one v3 priv read all-items`
		`switch(config)#`
		Configuring the User
		An SNMP user is a member of an SNMP group. The snmp-server user command adds a new user to an SNMP group and configures that user's parameters. To configure a remote user, specify the IP address or port number of the device where the user's remote SNMP agent resides.
		
		Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1966.
		
		See also Arista User Manual v. 4.13.6F (4/14/2014), at 1894; Arista User Manual v. 4.12.3 (7/17/13), at 1656; Arista User Manual, v. 4.11.1 (1/11/13), at 1343-44; Arista User Manual v. 4.10.3 (10/22/12), at 1109-10; Arista User Manual v. 4.9.3.2 (5/3/12), at 865; Arista User Manual v. 4.8.2 (11/18/11), at 677; Arista User Manual v. 4.7.3 (7/18/11), at 533.

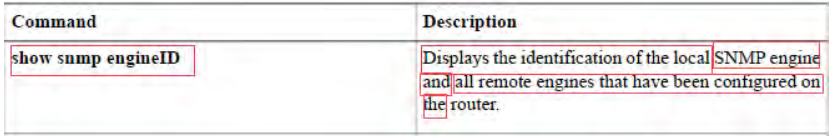
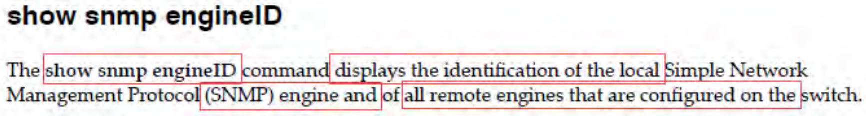
Copyright Registration Information	Cisco	Arista

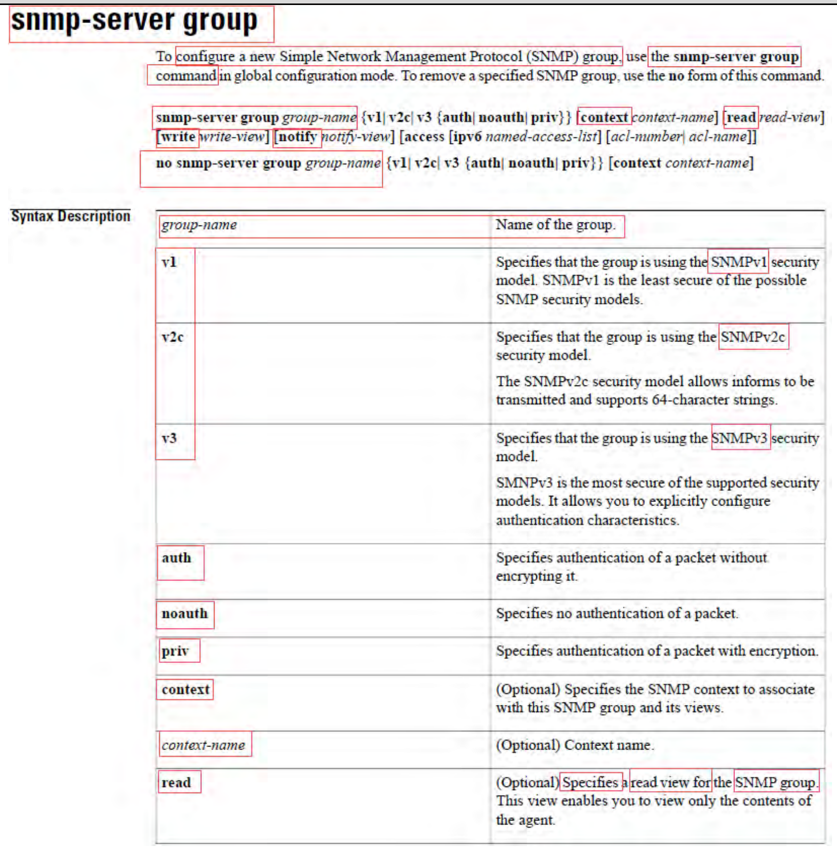
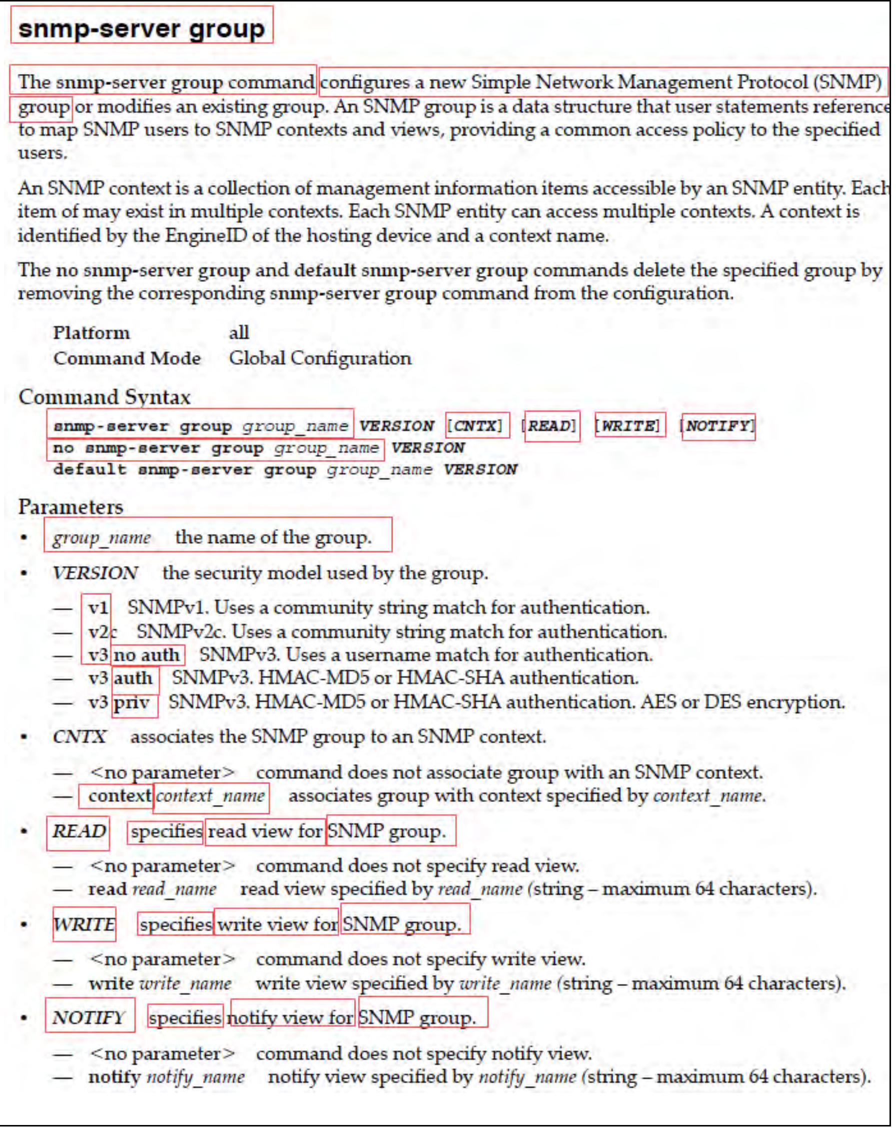
Cisco IOS 15.4
Effective date of registration: 11/26/2014
	
	snmp trap link-status
	To enable Simple Network Management Protocol (SNMP) link trap generation, use the **snmp trap link-status** command in either interface configuration mode or service instance configuration mode. To disable SNMP link trap generation, use the **no** form of this command.
	snmp trap link-status [**permit duplicates**]
	no snmp trap link-status [**permit duplicates**]
	Cisco IOS SNMP Support Command Reference (2013), at 130.
		
		snmp trap link-status
		The **snmp trap link-status** command enables Simple Network Management Protocol (SNMP) link-status trap generation on the configuration mode interface. The generation of link-status traps is enabled by default. If SNMP link-trap generation was previously disabled, this command removes the corresponding **no snmp link-status** statement from the configuration to re-enable link-trap generation.
		The **no snmp trap link-status** command disables SNMP link trap generation on the configuration mode interface.
		The **snmp trap link-status** and **default snmp trap link-status** commands restore the default behavior by removing the **no snmp trap link-status** command from *running-config*. Only the no form of this command is visible in *running-config*.
		Platform all
		Command Mode Interface-Ethernet Configuration
		Interface-Loopback Configuration
		Interface-Management Configuration
		Interface-Port-channel Configuration
		Interface-VLAN Configuration
		Interface-VXLAN Configuration
		Command Syntax
		`snmp trap link-status`
		`no snmp trap link-status`
		`default snmp trap link-status`
		Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1966.
		See also Arista User Manual v. 4.12.3 (7/17/13), at 1692; Arista User Manual, v. 4.11.1 (1/11/13), at 1377; Arista User Manual v. 4.10.3 (10/22/12), at 1144; Arista User Manual v. 4.9.3.2 (5/3/12), at 898; Arista User Manual v. 4.8.2 (11/18/11), at 705; Arista User Manual v. 4.7.3 (7/18/11), at 561.

Copyright Registration Information	Cisco	Arista
Cisco IOS 15.4 Effective date of registration: 11/26/2014	 snmp-server host Specifies the targeted recipient of an SNMP notification operation. Cisco IOS SNMP Support Command Reference (2013), at 191.	 **Configuring the Host** The snmp-server host command specifies the recipient of a SNMP notification. An SNMP host is the recipient of an SNMP trap operation. The snmp-server host command sets the community string if i was not previously configured. Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1967. *See also* Arista User Manual v. 4.13.6F (4/14/2014), at 1895; Arista User Manual v. 4.12.3 (7/17/13), at 1656; Arista User Manual, v. 4.11.1 (1/11/13), at 1344; Arista User Manual v. 4.10.3 (10/22/12), at 1110; Arista User Manual v. 4.9.3.2 (5/3/12), at 866; Arista User Manual v. 4.8.2 (11/18/11), at 677; Arista User Manual v. 4.7.3 (7/18/11), at 533.
Cisco IOS 15.4 Effective date of registration: 11/26/2014	 **Usage Guidelines** SNMP notifications can be sent as traps or inform requests. This command enables both traps and inform requests. Cisco IOS SNMP Support Command Reference (2013), at 216.	 The snmp-server enable traps command enables the transmission of Simple Network Management Protocol (SNMP) notifications as traps or inform requests. This command enables both traps and infor requests for the specified notification types. The snmp-server host command specifies the notificatio type (traps or informs). Sending notifications requires at least one snmp-server host command. Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1990. *See also* Arista User Manual v. 4.12.3 (7/17/13), at 1680; Arista User Manual, v. 4.11.1 (1/11/13), at 1365; Arista User Manual v. 4.10.3 (10/22/12), at 1132; Arista User Manual v. 4.9.3.2 (5/3/12), at 888; Arista User Manual v. 4.8.2 at 696; Arista User Manual v. 4.7.3 (7/18/11), at 552.

Copyright Registration Information	Cisco	Arista

Cisco IOS 15.4
 	
Effective date of registration: 11/26/2014
	
	snmp-server engineID local
	To specify the Simple Network Management Protocol (SNMP) engine ID on the local device, use the **snmp-server engineID local** command in global configuration mode. To remove the configured engine ID, use the **no** form of this command.
	snmp-server engineID local *engineid-string*
	no snmp-server engineID local *engineid-string*
	Syntax Description — *engineid-string* — String of a maximum of 24 characters that identifies the engine ID.
	Command Default — An SNMP engine ID is generated automatically but is not displayed or stored in the running configuration. You can display the default or configured engine ID by using the **show snmp engineID** command.
	Command Modes — Global configuration (config)
	Command History
	Release — Modification
	12.0(3)T — This command was introduced.
	12.2(33)SRA — This command was integrated into Cisco IOS Release 12.2(33)SRA.
	12.2SX — This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
	Usage Guidelines — The SNMP engine ID is a unique string used to identify the device for administrative purposes. You do not need to specify an engine ID for the device; a default string is generated using Cisco's enterprise number (1.3.6.1.4.1.9) and the MAC address of the first interface on the device. For further details on the SNMP engine ID, see RFC 2571.
	If you specify your own ID, note that the entire 24-character engine ID is not needed if it contains trailing zeros. Specify only the portion of the engine ID up until the point where only zeros remain in the value. For example, to configure an engine ID of 123400000000000000000000, you can specify **snmp-server engineID local 1234**.
	The value for the engine ID is displayed in hexadecimal value pairs. If the length of the input is an odd number, the last digit will be prepended with a zero ("0"). For example, if the engine ID is 12345, the ID is treated as 12:34:05 internally. Hence, the engine ID is displayed as 123405 in the **show running configuration** command output.
	Changing the value of the SNMP engine ID has significant effects. A user's password (entered on the command line) is converted to a message digest5 algorithm (MD5) or Secure Hash Algorithm (SHA) security digest. This digest is based on both the password and the local engine ID. The command line password is then destroyed, as required by RFC 2274. Because of this deletion, if the local value of the engineID changes, the security digests of SNMPv3 users will become invalid, and the users will have to be reconfigured.
	Similar restrictions require the reconfiguration of community strings when the engine ID changes. A remote engine ID is required when an SNMPv3 inform is configured. The remote engine ID is used to compute the security digest for authenticating and encrypting packets sent to a user on the remote host.
	Examples — The following example specifies the local SNMP engine ID:
	`Router(config)# snmp-server engineID local`
	
	Cisco IOS SNMP Support Command Reference (2013), at 339-340.
		
		snmp-server engineID local
		The snmp-server engineID local command configures the name for the local Simple Network Management Protocol (SNMP) engine. The default SNMP engineID is generated by the switch and is used when an engineID is not configured with this command. The show snmp engineID command displays the default or configured engine ID.
		SNMPv3 authenticates users through security digests (MD5 or SHA) that are based on user passwords and the local engine ID. Passwords entered on the CLI are similarly converted, then compared to the user's security digest to authenticate the user.
		Important — Changing the local engineID value invalidates SNMPv3 security digests, requiring the reconfiguration of all user passwords.
		The no snmp-server engineID and default snmp-server engineID commands restore the default engineID by removing the snmp-server engineID command from the configuration.
		Platform — all
		Command Mode — Global Configuration
		Command Syntax
		`snmp-server engineID local` *`engine_hex`*
		`no snmp-server engineID local`
		`default snmp-server engineID`
		Parameters
		• *engine_hex* — the switch's name for the local SNMP engine (hex string). The string must consist of at least ten characters with a maximum of 64 characters.
		Example
		• This command configures DC945798CAB4 as the name of the local SNMP engine.
		`switch(config)#snmp-server engineID local DC945798CAB4`
		`switch(config)#`
		snmp-server engineID remote
		The snmp-server engineID remote command configures the name of a Simple Network Management Protocol (SNMP) engine located on a remote device. The switch generates a default engineID; use the show snmp engineID command to view the configured or default engineID.
		A remote engine ID is required when configuring an SNMPv3 inform to compute the security digest for authenticating and encrypting packets sent to users on the remote host. SNMPv3 authenticates users through security digests (MD5 or SHA) that are based on user passwords and the engine ID. Passwords entered on the CLI are similarly converted, then compared to the user's security digest to authenticate the user.
		
		Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1991-92.
		
		See also Arista User Manual v. 4.12.3 (7/17/13), at 1681-82; Arista User Manual, v. 4.11.1 (1/11/13), at 1366-67; Arista User Manual v. 4.10.3 (10/22/12), at 1133-34; Arista User Manual v. 4.9.3.2 (5/3/12), at 889-890; Arista User Manual v. 4.8.2 (11/18/11), at 697-98; Arista User

Copyright Registration Information	Cisco	Arista
		Manual v. 4.7.3 (7/18/11), at 553-54.
Cisco IOS 15.4 Effective date of registration: 11/26/2014	 **Command** — **Description** **show snmp engineID** — Displays the identification of the local SNMP engine and all remote engines that have been configured on the router. Cisco IOS SNMP Support Command Reference (2013), at 340/	 **show snmp engineID** The show snmp engineID command displays the identification of the local Simple Network Management Protocol (SNMP) engine and of all remote engines that are configured on the switch. Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1978. *See also* Arista User Manual v. 4.12.3 (7/17/13), at 1668; Arista User Manual, v. 4.11.1 (1/11/13), at 1355; Arista User Manual v. 4.10.3 (10/22/12), at 1122; Arista User Manual v. 4.9.3.2 (5/3/12), at 878; Arista User Manual v. 4.8.2 (11/18/11), at 686; Arista User Manual v. 4.7.3 (7/18/11), at 542.

Copyright Registration Information	Cisco	Arista
Cisco IOS 15.4 Effective date of registration: 11/26/2014		

snmp-server group

To configure a new Simple Network Management Protocol (SNMP) group, use the **snmp-server group** command in global configuration mode. To remove a specified SNMP group, use the **no** form of this command.

snmp-server group *group-name* {**v1**| **v2c**| **v3** {**auth**| **noauth**| **priv**}} [**context** *context-name*] [**read** *read-view*] [**write** *write-view*] [**notify** *notify-view*] [**access** [**ipv6** *named-access-list*] [*acl-number*| *acl-name*]]

no snmp-server group *group-name* {**v1**| **v2c**| **v3** {**auth**| **noauth**| **priv**}} [**context** *context-name*]

Syntax Description

group-name	Name of the group.
v1	Specifies that the group is using the SNMPv1 security model. SNMPv1 is the least secure of the possible SNMP security models.
v2c	Specifies that the group is using the SNMPv2c security model. The SNMPv2c security model allows informs to be transmitted and supports 64-character strings.
v3	Specifies that the group is using the SNMPv3 security model. SMNPv3 is the most secure of the supported security models. It allows you to explicitly configure authentication characteristics.
auth	Specifies authentication of a packet without encrypting it.
noauth	Specifies no authentication of a packet.
priv	Specifies authentication of a packet with encryption.
context	(Optional) Specifies the SNMP context to associate with this SNMP group and its views.
context-name	(Optional) Context name.
read	(Optional) Specifies a read view for the SNMP group. This view enables you to view only the contents of the agent.

snmp-server group

The **snmp-server group** command configures a new Simple Network Management Protocol (SNMP) group or modifies an existing group. An SNMP group is a data structure that user statements reference to map SNMP users to SNMP contexts and views, providing a common access policy to the specified users.

An SNMP context is a collection of management information items accessible by an SNMP entity. Each item of may exist in multiple contexts. Each SNMP entity can access multiple contexts. A context is identified by the EngineID of the hosting device and a context name.

The **no snmp-server group** and **default snmp-server group** commands delete the specified group by removing the corresponding **snmp-server group** command from the configuration.

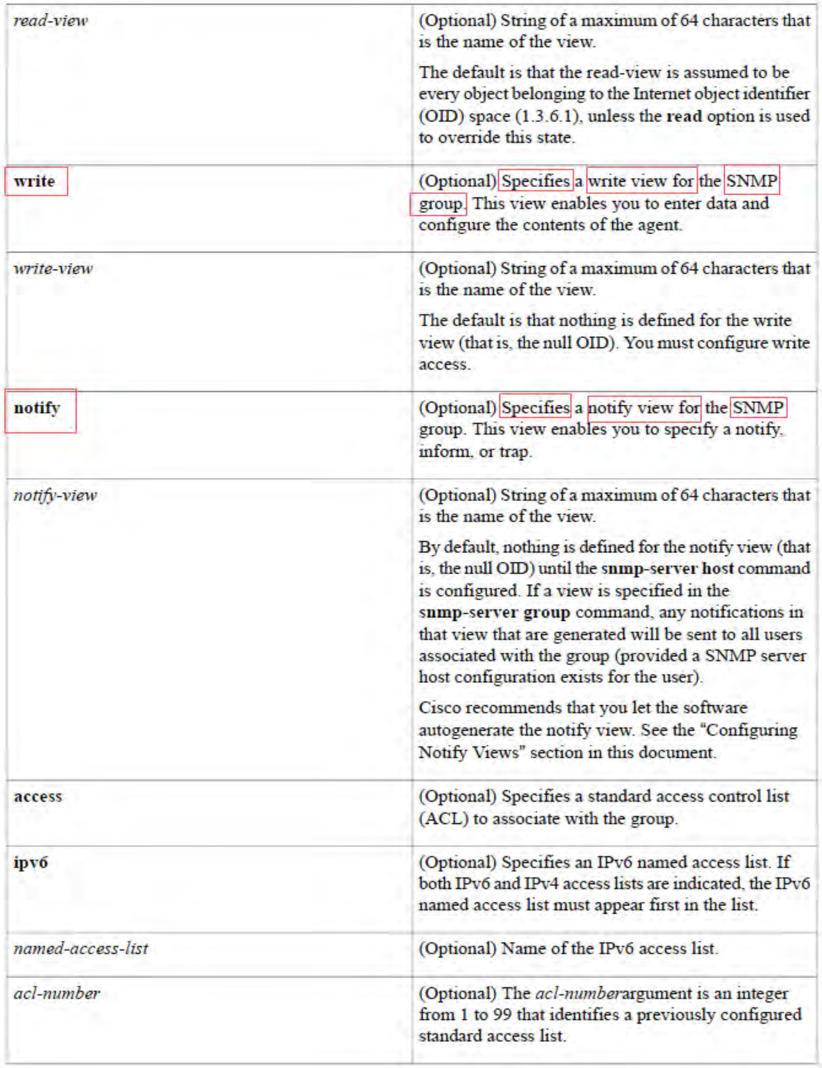
Platform	all
Command Mode	Global Configuration

Command Syntax

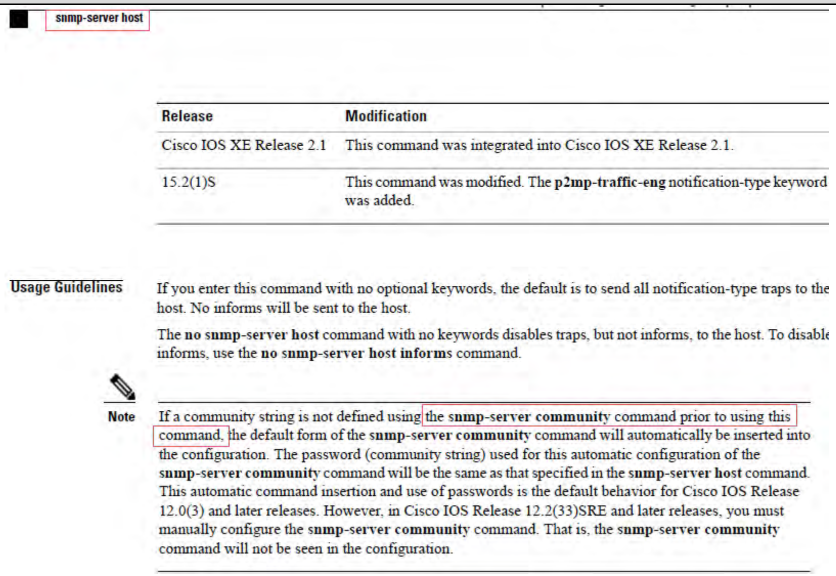
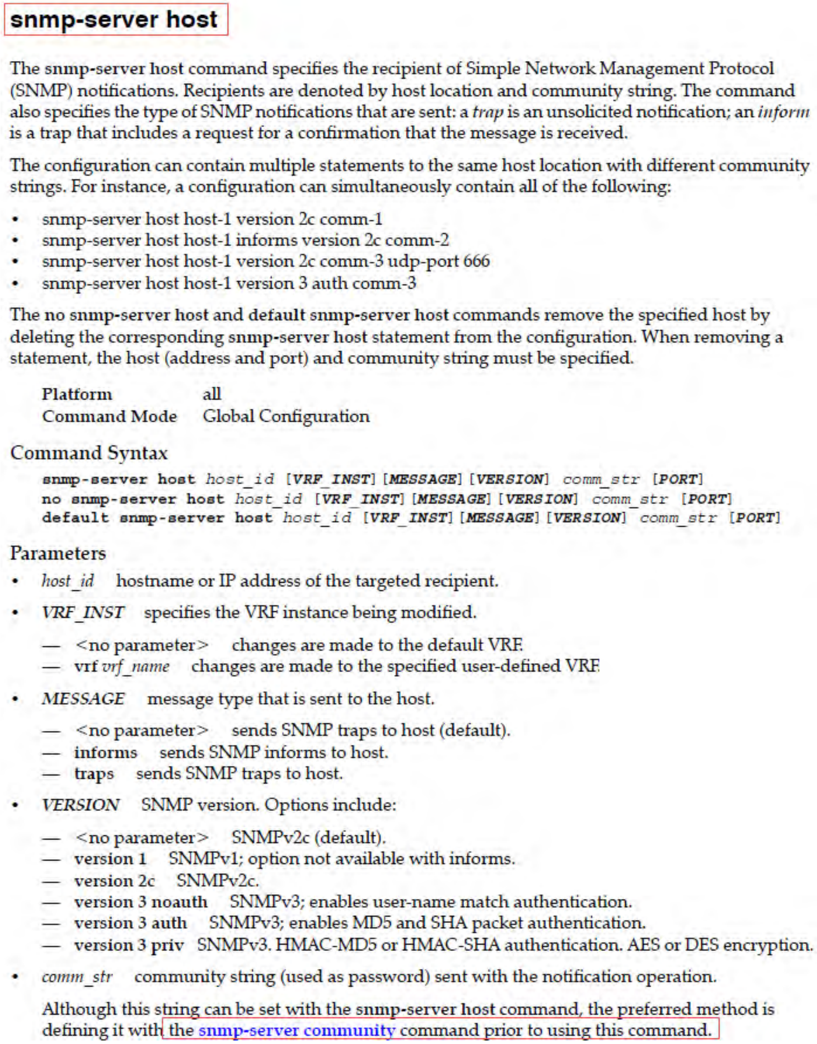
```
snmp-server group group_name VERSION [CNTX] [READ] [WRITE] [NOTIFY]
no snmp-server group group_name VERSION
default snmp-server group group_name VERSION
```

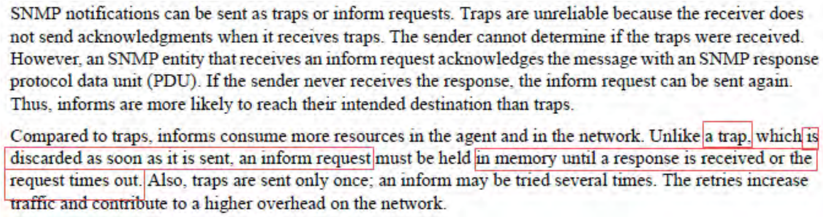
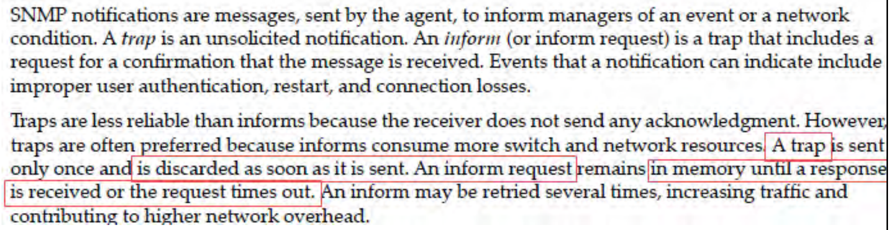
Parameters

- *group_name* the name of the group.
- *VERSION* the security model used by the group.
  - — **v1** SNMPv1. Uses a community string match for authentication.
  - — **v2c** SNMPv2c. Uses a community string match for authentication.
  - — **v3 no auth** SNMPv3. Uses a username match for authentication.
  - — **v3 auth** SNMPv3. HMAC-MD5 or HMAC-SHA authentication.
  - — **v3 priv** SNMPv3. HMAC-MD5 or HMAC-SHA authentication. AES or DES encryption.
- *CNTX* associates the SNMP group to an SNMP context.
  - — <no parameter> command does not associate group with an SNMP context.
  - — **context** *context_name* associates group with context specified by *context_name*.
- *READ* specifies read view for SNMP group.
  - — <no parameter> command does not specify read view.
  - — **read** *read_name* read view specified by *read_name* (string – maximum 64 characters).
- *WRITE* specifies write view for SNMP group.
  - — <no parameter> command does not specify write view.
  - — **write** *write_name* write view specified by *write_name* (string – maximum 64 characters).
- *NOTIFY* specifies notify view for SNMP group.
  - — <no parameter> command does not specify notify view.
  - — **notify** *notify_name* notify view specified by *notify_name* (string – maximum 64 characters).

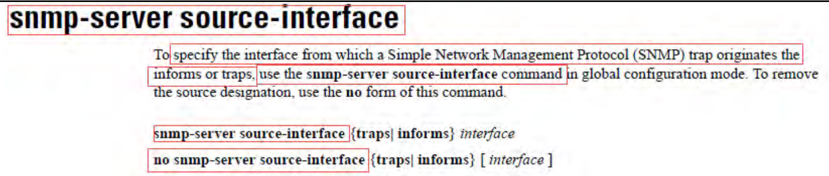
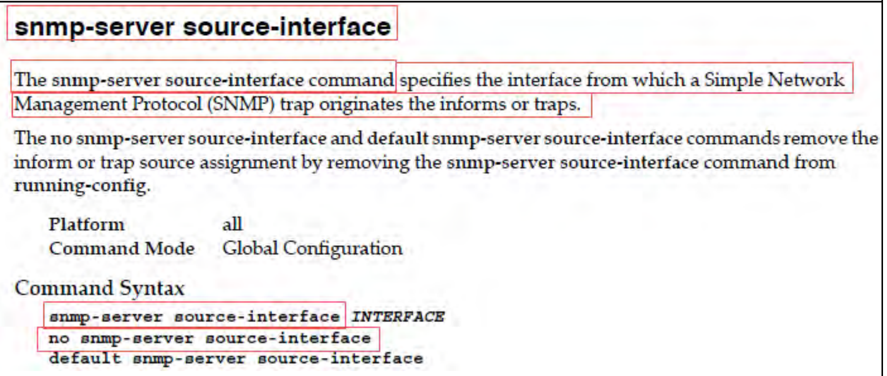
<table>
<tr><th>Copyright Registration Information</th><th>Cisco</th><th>Arista</th></tr>
<tr>
<td>Cisco IOS 15.4
Effective date of registration: 11/26/2014</td>
<td>

<table>
<tr><td><i>read-view</i></td><td>(Optional) String of a maximum of 64 characters that is the name of the view.
The default is that the read-view is assumed to be every object belonging to the Internet object identifier (OID) space (1.3.6.1), unless the <b>read</b> option is used to override this state.</td></tr>
<tr><td><b>write</b></td><td>(Optional) Specifies a write view for the SNMP group. This view enables you to enter data and configure the contents of the agent.</td></tr>
<tr><td><i>write-view</i></td><td>(Optional) String of a maximum of 64 characters that is the name of the view.
The default is that nothing is defined for the write view (that is, the null OID). You must configure write access.</td></tr>
<tr><td><b>notify</b></td><td>(Optional) Specifies a notify view for the SNMP group. This view enables you to specify a notify, inform, or trap.</td></tr>
<tr><td><i>notify-view</i></td><td>(Optional) String of a maximum of 64 characters that is the name of the view.
By default, nothing is defined for the notify view (that is, the null OID) until the <b>snmp-server host</b> command is configured. If a view is specified in the <b>snmp-server group</b> command, any notifications in that view that are generated will be sent to all users associated with the group (provided a SNMP server host configuration exists for the user).
Cisco recommends that you let the software autogenerate the notify view. See the "Configuring Notify Views" section in this document.</td></tr>
<tr><td><b>access</b></td><td>(Optional) Specifies a standard access control list (ACL) to associate with the group.</td></tr>
<tr><td><b>ipv6</b></td><td>(Optional) Specifies an IPv6 named access list. If both IPv6 and IPv4 access lists are indicated, the IPv6 named access list must appear first in the list.</td></tr>
<tr><td><i>named-access-list</i></td><td>(Optional) Name of the IPv6 access list.</td></tr>
<tr><td><i>acl-number</i></td><td>(Optional) The <i>acl-number</i>argument is an integer from 1 to 99 that identifies a previously configured standard access list.</td></tr>
</table>
Cisco IOS SNMP Support Command Reference (2013), at 343-44.
</td>
<td>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1994.
<i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 1684; Arista User Manual, v. 4.11.1 (1/11/13), at 1369; Arista User Manual v. 4.10.3 (10/22/12), at 1136; Arista User Manual v. 4.9.3.2 (5/3/12), at 892; Arista User Manual v. 4.8.2 (11/18/11), at 699; Arista User Manual v. 4.7.3 (7/18/11), at 555.</td>
</tr>
</table>

Copyright Registration Information	Cisco	Arista

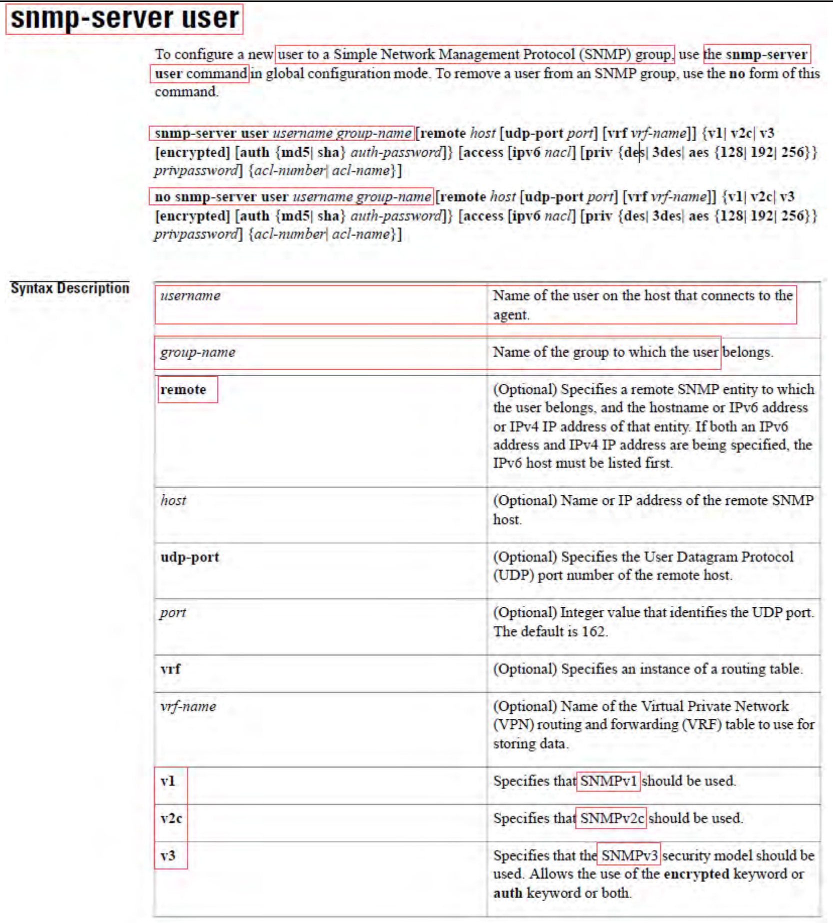
Cisco IOS 15.4
 	
Effective date of registration: 11/26/2014
	
	snmp-server host
	
	Release **Modification**
	Cisco IOS XE Release 2.1 This command was integrated into Cisco IOS XE Release 2.1.
	15.2(1)S This command was modified. The **p2mp-traffic-eng** notification-type keyword was added.
	
	Usage Guidelines If you enter this command with no optional keywords, the default is to send all notification-type traps to the host. No informs will be sent to the host.
	
	The **no snmp-server host** command with no keywords disables traps, but not informs, to the host. To disable informs, use the **no snmp-server host informs** command.
	
	Note If a community string is not defined using the **snmp-server community** command prior to using this command, the default form of the **snmp-server community** command will automatically be inserted into the configuration. The password (community string) used for this automatic configuration of the **snmp-server community** command will be the same as that specified in the **snmp-server host** command. This automatic command insertion and use of passwords is the default behavior for Cisco IOS Release 12.0(3) and later releases. However, in Cisco IOS Release 12.2(33)SRE and later releases, you must manually configure the **snmp-server community** command. That is, the **snmp-server community** command will not be seen in the configuration.
	
	Cisco IOS SNMP Support Command Reference (2013), at 354.
		
		snmp-server host
		
		The **snmp-server host** command specifies the recipient of Simple Network Management Protocol (SNMP) notifications. Recipients are denoted by host location and community string. The command also specifies the type of SNMP notifications that are sent: a *trap* is an unsolicited notification; an *inform* is a trap that includes a request for a confirmation that the message is received.
		
		The configuration can contain multiple statements to the same host location with different community strings. For instance, a configuration can simultaneously contain all of the following:
		• snmp-server host host-1 version 2c comm-1
		• snmp-server host host-1 informs version 2c comm-2
		• snmp-server host host-1 version 2c comm-3 udp-port 666
		• snmp-server host host-1 version 3 auth comm-3
		
		The **no snmp-server host** and **default snmp-server host** commands remove the specified host by deleting the corresponding **snmp-server host** statement from the configuration. When removing a statement, the host (address and port) and community string must be specified.
		
		Platform all
		Command Mode Global Configuration
		
		Command Syntax
		`snmp-server host host_id [VRF_INST] [MESSAGE] [VERSION] comm_str [PORT]`
		`no snmp-server host host_id [VRF_INST] [MESSAGE] [VERSION] comm_str [PORT]`
		`default snmp-server host host_id [VRF_INST] [MESSAGE] [VERSION] comm_str [PORT]`
		
		Parameters
		• *host_id* hostname or IP address of the targeted recipient.
		• *VRF_INST* specifies the VRF instance being modified.
		— <no parameter> changes are made to the default VRF.
		— **vrf** *vrf_name* changes are made to the specified user-defined VRF.
		• *MESSAGE* message type that is sent to the host.
		— <no parameter> sends SNMP traps to host (default).
		— **informs** sends SNMP informs to host.
		— **traps** sends SNMP traps to host.
		• *VERSION* SNMP version. Options include:
		— <no parameter> SNMPv2c (default).
		— **version 1** SNMPv1; option not available with informs.
		— **version 2c** SNMPv2c.
		— **version 3 noauth** SNMPv3; enables user-name match authentication.
		— **version 3 auth** SNMPv3; enables MD5 and SHA packet authentication.
		— **version 3 priv** SNMPv3. HMAC-MD5 or HMAC-SHA authentication. AES or DES encryption.
		• *comm_str* community string (used as password) sent with the notification operation.
		Although this string can be set with the **snmp-server host** command, the preferred method is defining it with the **snmp-server community** command prior to using this command.
		
		Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1995.
		
		See also Arista User Manual v. 4.12.3 (7/17/13), at 1685; Arista User

Copyright Registration Information	Cisco	Arista
		Manual, v. 4.11.1 (1/11/13), at 1370; Arista User Manual v. 4.10.3 (10/22/12), at 1137; Arista User Manual v. 4.9.3.2 (5/3/12), at 893; Arista User Manual v. 4.8.2 (11/18/11), at 700; Arista User Manual v. 4.7.3 (7/18/11), at 556.
Cisco IOS 15.4 Effective date of registration: 11/26/2014	 SNMP notifications can be sent as traps or inform requests. Traps are unreliable because the receiver does not send acknowledgments when it receives traps. The sender cannot determine if the traps were received. However, an SNMP entity that receives an inform request acknowledges the message with an SNMP response protocol data unit (PDU). If the sender never receives the response, the inform request can be sent again. Thus, informs are more likely to reach their intended destination than traps. Compared to traps, informs consume more resources in the agent and in the network. Unlike a trap, which is discarded as soon as it is sent, an inform request must be held in memory until a response is received or the request times out. Also, traps are sent only once; an inform may be tried several times. The retries increase traffic and contribute to a higher overhead on the network. Cisco IOS SNMP Support Command Reference (2013), at 354.	 SNMP notifications are messages, sent by the agent, to inform managers of an event or a network condition. A *trap* is an unsolicited notification. An *inform* (or inform request) is a trap that includes a request for a confirmation that the message is received. Events that a notification can indicate include improper user authentication, restart, and connection losses. Traps are less reliable than informs because the receiver does not send any acknowledgment. However, traps are often preferred because informs consume more switch and network resources. A trap is sent only once and is discarded as soon as it is sent. An inform request remains in memory until a response is received or the request times out. An inform may be retried several times, increasing traffic and contributing to higher network overhead. Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1963. *See also* Arista User Manual v. 4.13.6F (4/14/2014), at 1891; Arista User Manual v. 4.12.3 (7/17/13), at 1653; Arista User Manual, v. 4.11.1 (1/11/13), at 1341; Arista User Manual v. 4.10.3 (10/22/12), at 1107; Arista User Manual v. 4.9.3.2 (5/3/12), at 863; Arista User Manual v. 4.8.2 at 675; Arista User Manual v. 4.7.3 (7/18/11), at 531.

Copyright Registration Information	Cisco	Arista

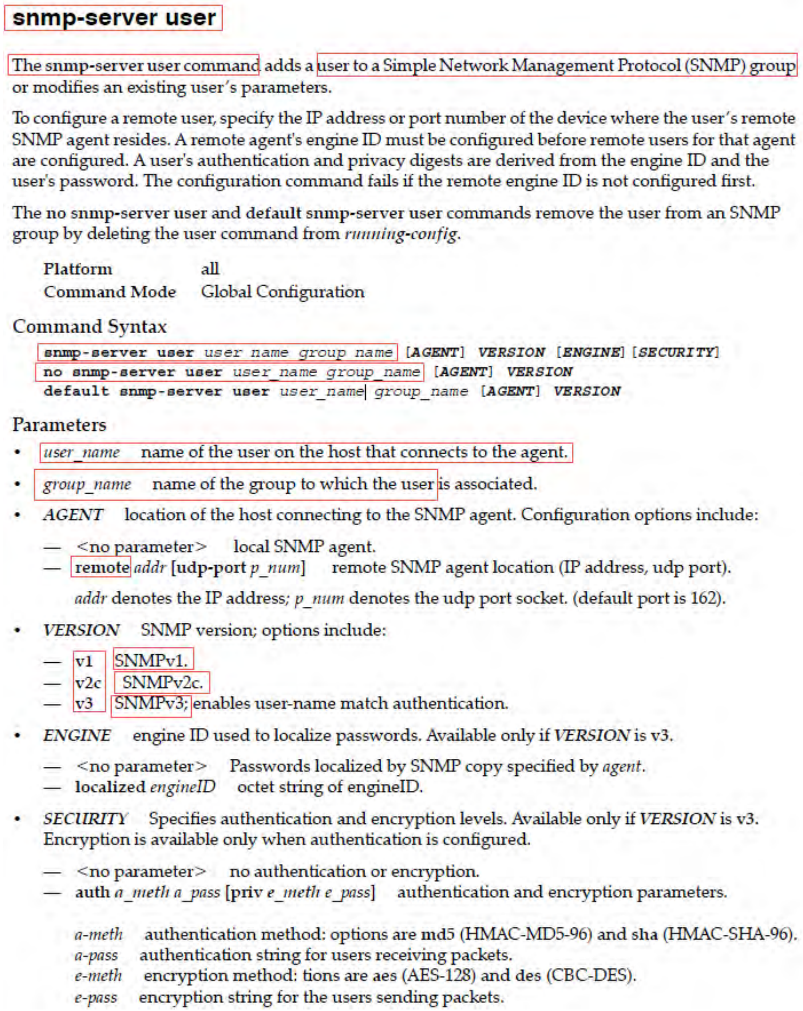
Cisco IOS 15.4
Effective date of registration: 11/26/2014
	
	snmp-server source-interface
	To specify the interface from which a Simple Network Management Protocol (SNMP) trap originates the informs or traps, use the **snmp-server source-interface** command in global configuration mode. To remove the source designation, use the **no** form of this command.
	snmp-server source-interface {**traps**| **informs**} *interface*
	no snmp-server source-interface {**traps**| **informs**} [*interface*]
	Cisco IOS SNMP Support Command Reference (2013), at 376.
		
		snmp-server source-interface
		The snmp-server source-interface command specifies the interface from which a Simple Network Management Protocol (SNMP) trap originates the informs or traps.
		The no snmp-server source-interface and default snmp-server source-interface commands remove the inform or trap source assignment by removing the snmp-server source-interface command from running-config.
		Platform all
		Command Mode Global Configuration
		Command Syntax
		`snmp-server source-interface` ***INTERFACE***
		`no snmp-server source-interface`
		`default snmp-server source-interface`
		Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1967.
		See also Arista User Manual v. 4.12.3 (7/17/13), at 1688; Arista User Manual, v. 4.11.1 (1/11/13), at 1373; Arista User Manual v. 4.10.3 (10/22/12), at 1140; Arista User Manual v. 4.9.3.2 (5/3/12), at 895; Arista User Manual v. 4.8.2 (11/18/11), at 702; Arista User Manual v. 4.7.3 (7/18/11), at 558.

<table>
<tr><th>Copyright Registration Information</th><th>Cisco</th><th>Arista</th></tr>
<tr>
<td>Cisco IOS 15.4

Effective date of registration: 11/26/2014</td>
<td>
<b>snmp-server user</b>
To configure a new user to a Simple Network Management Protocol (SNMP) group, use the <b>snmp-server user</b> command in global configuration mode. To remove a user from an SNMP group, use the <b>no</b> form of this command.

<b>snmp-server user</b> <i>username group-name</i> [<b>remote</b> <i>host</i> [<b>udp-port</b> <i>port</i>] [<b>vrf</b> <i>vrf-name</i>]] {<b>v1</b>| <b>v2c</b>| <b>v3</b> [<b>encrypted</b>] [<b>auth</b> {<b>md5</b>| <b>sha</b>} <i>auth-password</i>]} [<b>access</b> [<b>ipv6</b> <i>nacl</i>] [<b>priv</b> {<b>des</b>| <b>3des</b>| <b>aes</b> {<b>128</b>| <b>192</b>| <b>256</b>}} <i>privpassword</i>] {<i>acl-number</i>| <i>acl-name</i>}]
<b>no snmp-server user</b> <i>username group-name</i> [<b>remote</b> <i>host</i> [<b>udp-port</b> <i>port</i>] [<b>vrf</b> <i>vrf-name</i>]] {<b>v1</b>| <b>v2c</b>| <b>v3</b> [<b>encrypted</b>] [<b>auth</b> {<b>md5</b>| <b>sha</b>} <i>auth-password</i>]} [<b>access</b> [<b>ipv6</b> <i>nacl</i>] [<b>priv</b> {<b>des</b>| <b>3des</b>| <b>aes</b> {<b>128</b>| <b>192</b>| <b>256</b>}} <i>privpassword</i>] {<i>acl-number</i>| <i>acl-name</i>}]

<b>Syntax Description</b>
<table>
<tr><td><i>username</i></td><td>Name of the user on the host that connects to the agent.</td></tr>
<tr><td><i>group-name</i></td><td>Name of the group to which the user belongs.</td></tr>
<tr><td><b>remote</b></td><td>(Optional) Specifies a remote SNMP entity to which the user belongs, and the hostname or IPv6 address or IPv4 IP address of that entity. If both an IPv6 address and IPv4 IP address are being specified, the IPv6 host must be listed first.</td></tr>
<tr><td><i>host</i></td><td>(Optional) Name or IP address of the remote SNMP host.</td></tr>
<tr><td><b>udp-port</b></td><td>(Optional) Specifies the User Datagram Protocol (UDP) port number of the remote host.</td></tr>
<tr><td><i>port</i></td><td>(Optional) Integer value that identifies the UDP port. The default is 162.</td></tr>
<tr><td><b>vrf</b></td><td>(Optional) Specifies an instance of a routing table.</td></tr>
<tr><td><i>vrf-name</i></td><td>(Optional) Name of the Virtual Private Network (VPN) routing and forwarding (VRF) table to use for storing data.</td></tr>
<tr><td><b>v1</b></td><td>Specifies that SNMPv1 should be used.</td></tr>
<tr><td><b>v2c</b></td><td>Specifies that SNMPv2c should be used.</td></tr>
<tr><td><b>v3</b></td><td>Specifies that the SNMPv3 security model should be used. Allows the use of the <b>encrypted</b> keyword or <b>auth</b> keyword or both.</td></tr>
</table>

Cisco IOS SNMP Support Command Reference (2013), at 394.</td>
<td>
<b>snmp-server user</b>
The snmp-server user command adds a user to a Simple Network Management Protocol (SNMP) group or modifies an existing user's parameters.

To configure a remote user, specify the IP address or port number of the device where the user's remote SNMP agent resides. A remote agent's engine ID must be configured before remote users for that agent are configured. A user's authentication and privacy digests are derived from the engine ID and the user's password. The configuration command fails if the remote engine ID is not configured first.

The no snmp-server user and default snmp-server user commands remove the user from an SNMP group by deleting the user command from <i>running-config</i>.

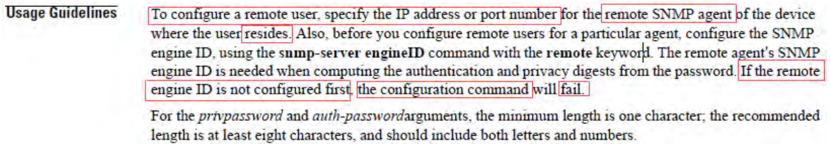
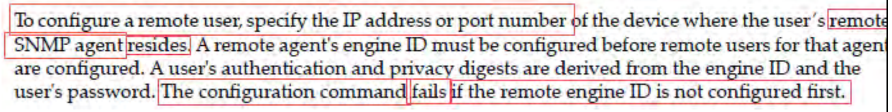
Platform all
Command Mode Global Configuration

Command Syntax
<code>snmp-server user <i>user name group name</i> [<i>AGENT</i>] <i>VERSION</i> [<i>ENGINE</i>] [<i>SECURITY</i>]</code>
<code>no snmp-server user <i>user_name group_name</i> [<i>AGENT</i>] <i>VERSION</i></code>
<code>default snmp-server user <i>user_name</i> <i>group_name</i> [<i>AGENT</i>] <i>VERSION</i></code>

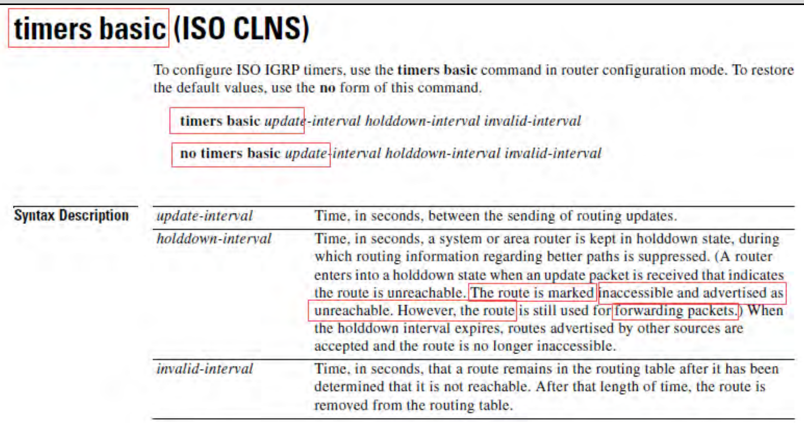
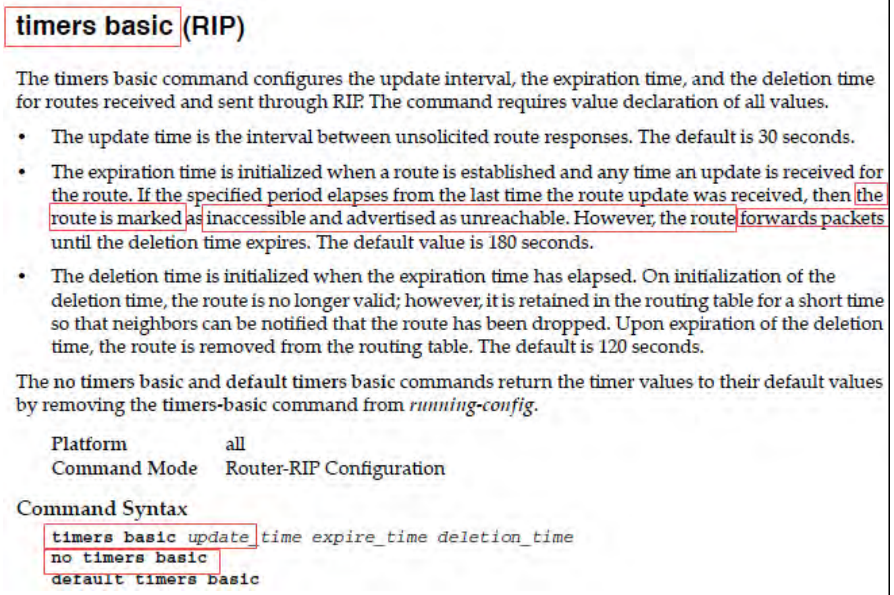
Parameters
• <i>user_name</i> name of the user on the host that connects to the agent.
• <i>group_name</i> name of the group to which the user is associated.
• <i>AGENT</i> location of the host connecting to the SNMP agent. Configuration options include:
— <no parameter> local SNMP agent.
— <b>remote</b> <i>addr</i> [<b>udp-port</b> <i>p_num</i>] remote SNMP agent location (IP address, udp port).
<i>addr</i> denotes the IP address; <i>p_num</i> denotes the udp port socket. (default port is 162).
• <i>VERSION</i> SNMP version; options include:
— <b>v1</b> SNMPv1.
— <b>v2c</b> SNMPv2c.
— <b>v3</b> SNMPv3; enables user-name match authentication.
• <i>ENGINE</i> engine ID used to localize passwords. Available only if <i>VERSION</i> is v3.
— <no parameter> Passwords localized by SNMP copy specified by <i>agent</i>.
— <b>localized</b> <i>engineID</i> octet string of engineID.
• <i>SECURITY</i> Specifies authentication and encryption levels. Available only if <i>VERSION</i> is v3. Encryption is available only when authentication is configured.
— <no parameter> no authentication or encryption.
— <b>auth</b> <i>a_meth a_pass</i> [<b>priv</b> <i>e_meth e_pass</i>] authentication and encryption parameters.
<i>a-meth</i> authentication method: options are md5 (HMAC-MD5-96) and sha (HMAC-SHA-96).
<i>a-pass</i> authentication string for users receiving packets.
<i>e-meth</i> encryption method: tions are aes (AES-128) and des (CBC-DES).
<i>e-pass</i> encryption string for the users sending packets.

Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1999.

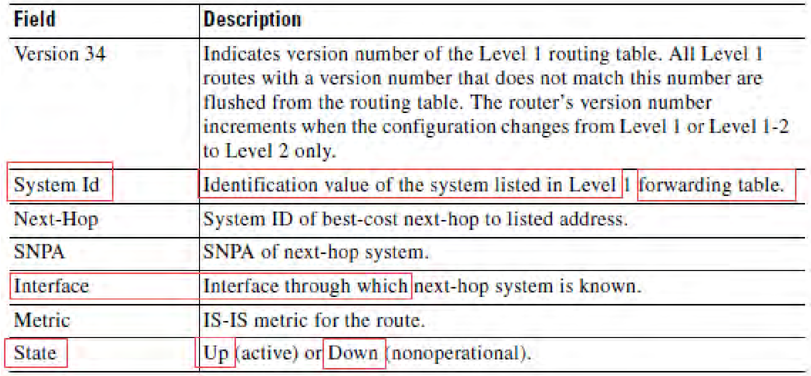
<i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 1689; Arista User Manual, v. 4.11.1 (1/11/13), at 1374; Arista User Manual v. 4.10.3</td>
</tr>
</table>

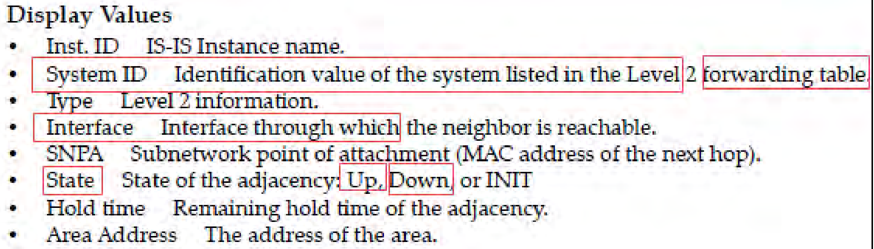
Copyright Registration Information	Cisco	Arista
		(10/22/12), at 1141; Arista User Manual v. 4.9.3.2 (5/3/12), at 896; Arista User Manual v. 4.8.2 (11/18/11), at 703; Arista User Manual v. 4.7.3 (7/18/11), at 559.
Cisco IOS 15.4 Effective date of registration: 11/26/2014	 **Usage Guidelines** To configure a remote user, specify the IP address or port number for the remote SNMP agent of the device where the user resides. Also, before you configure remote users for a particular agent, configure the SNMP engine ID, using the **snmp-server engineID** command with the **remote** keyword. The remote agent's SNMP engine ID is needed when computing the authentication and privacy digests from the password. If the remote engine ID is not configured first, the configuration command will fail. For the *privpassword* and *auth-password*arguments, the minimum length is one character; the recommended length is at least eight characters, and should include both letters and numbers. Cisco IOS SNMP Support Command Reference (2013), at 396.	 To configure a remote user, specify the IP address or port number of the device where the user's remote SNMP agent resides. A remote agent's engine ID must be configured before remote users for that agent are configured. A user's authentication and privacy digests are derived from the engine ID and the user's password. The configuration command fails if the remote engine ID is not configured first. Arista User Manual v. 4.14.3F (Rev. 2) 10/2/2014), at 1999. *See also* Arista User Manual v. 4.12.3 (7/17/13), at 1689; Arista User Manual, v. 4.11.1 (1/11/13), at 1374; Arista User Manual v. 4.10.3 (10/22/12), at 1141; Arista User Manual v. 4.9.3.2 (5/3/12), at 896; Arista User Manual v. 4.8.2 (11/18/11), at 703; Arista User Manual v. 4.7.3 (7/18/11), at 559.

Copyright Registration Information	Cisco	Arista

Cisco IOS 15.4
Effective date of registration: 11/26/2014
	
	timers basic (ISO CLNS)
	To configure ISO IGRP timers, use the **timers basic** command in router configuration mode. To restore the default values, use the **no** form of this command.
	timers basic *update-interval holddown-interval invalid-interval*
	no timers basic *update-interval holddown-interval invalid-interval*
	Syntax Description
	update-interval — Time, in seconds, between the sending of routing updates.
	holddown-interval — Time, in seconds, a system or area router is kept in holddown state, during which routing information regarding better paths is suppressed. (A router enters into a holddown state when an update packet is received that indicates the route is unreachable. The route is marked inaccessible and advertised as unreachable. However, the route is still used for forwarding packets.) When the holddown interval expires, routes advertised by other sources are accepted and the route is no longer inaccessible.
	invalid-interval — Time, in seconds, that a route remains in the routing table after it has been determined that it is not reachable. After that length of time, the route is removed from the routing table.
	Cisco IOS Interface and Hardware Component Command Reference (2011), at ISO-178.
		
		timers basic (RIP)
		The timers basic command configures the update interval, the expiration time, and the deletion time for routes received and sent through RIP. The command requires value declaration of all values.
		• The update time is the interval between unsolicited route responses. The default is 30 seconds.
		• The expiration time is initialized when a route is established and any time an update is received for the route. If the specified period elapses from the last time the route update was received, then the route is marked as inaccessible and advertised as unreachable. However, the route forwards packets until the deletion time expires. The default value is 180 seconds.
		• The deletion time is initialized when the expiration time has elapsed. On initialization of the deletion time, the route is no longer valid; however, it is retained in the routing table for a short time so that neighbors can be notified that the route has been dropped. Upon expiration of the deletion time, the route is removed from the routing table. The default is 120 seconds.
		The no timers basic and default timers basic commands return the timer values to their default values by removing the timers-basic command from *running-config*.
		Platform all
		Command Mode Router-RIP Configuration
		Command Syntax
		`timers basic update_time expire_time deletion_time`
		`no timers basic`
		`default timers basic`
		Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1671.
		See also Arista User Manual v. 4.13.6F (4/14/2014), at 1621; Arista User Manual v. 4.12.3 (7/17/13), at 1433; Arista User Manual, v. 4.11.1 (1/11/13), at 1179; Arista User Manual v. 4.10.3 (10/22/12), at 989; Arista User Manual v. 4.9.3.2 (5/3/12), at 748; ; Arista User Manual v. 4.8.2 (11/18/11), at 570.

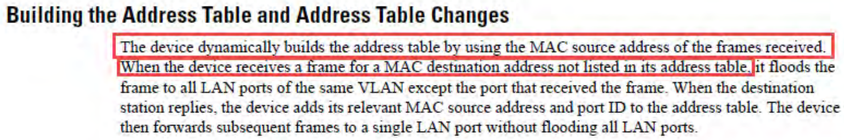
<table>
<tr><th>Copyright Registration Information</th><th>Cisco</th><th>Arista</th></tr>
<tr>
<td>Cisco IOS 15.4

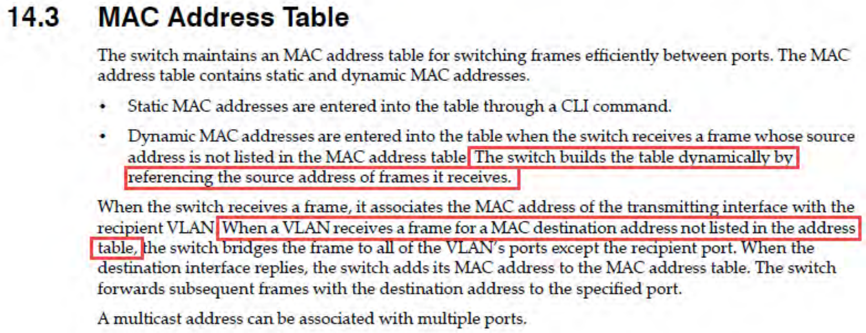
Effective date of registration: 11/26/2014</td>
<td>
<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Version 34</td><td>Indicates version number of the Level 1 routing table. All Level 1 routes with a version number that does not match this number are flushed from the routing table. The router's version number increments when the configuration changes from Level 1 or Level 1-2 to Level 2 only.</td></tr>
<tr><td>System Id</td><td>Identification value of the system listed in Level 1 forwarding table.</td></tr>
<tr><td>Next-Hop</td><td>System ID of best-cost next-hop to listed address.</td></tr>
<tr><td>SNPA</td><td>SNPA of next-hop system.</td></tr>
<tr><td>Interface</td><td>Interface through which next-hop system is known.</td></tr>
<tr><td>Metric</td><td>IS-IS metric for the route.</td></tr>
<tr><td>State</td><td>Up (active) or Down (nonoperational).</td></tr>
</table>

Cisco IOS Interface and Hardware Component Command Reference (2011), at ISO-137.</td>
<td>
Display Values
• Inst. ID IS-IS Instance name.
• System ID Identification value of the system listed in the Level 2 forwarding table.
• Type Level 2 information.
• Interface Interface through which the neighbor is reachable.
• SNPA Subnetwork point of attachment (MAC address of the next hop).
• State State of the adjacency: Up, Down, or INIT
• Hold time Remaining hold time of the adjacency.
• Area Address The address of the area.

Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1702.

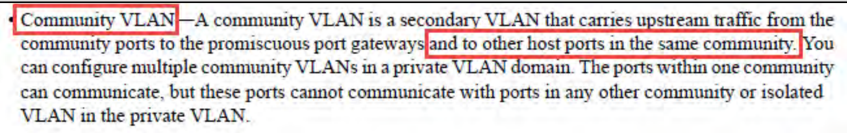
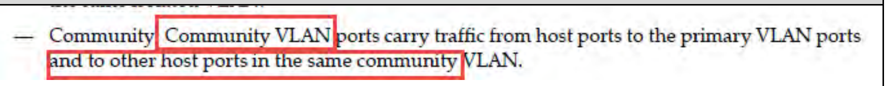
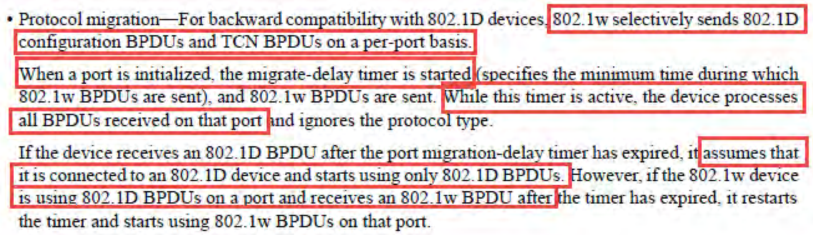
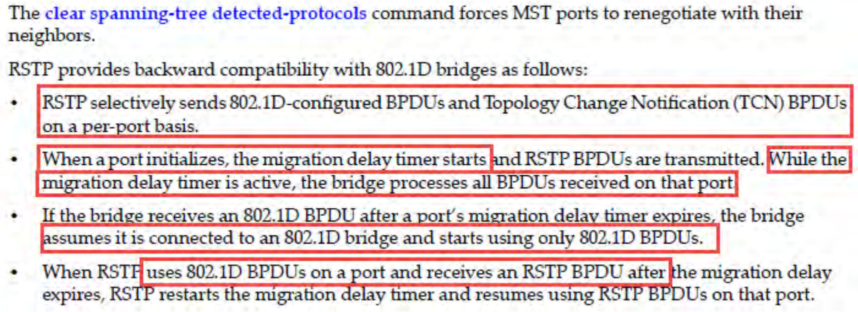
<i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 1459.</td>
</tr>
<tr>
<td>Cisco NX-OS 6.2

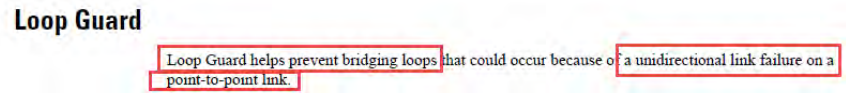
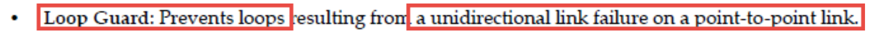
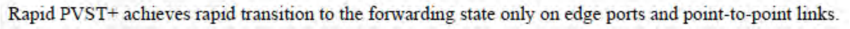
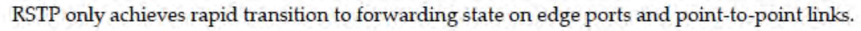
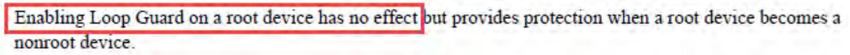
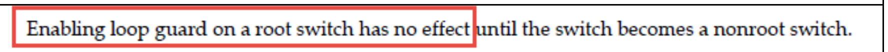
Effective date of registration: 11/13/2014</td>
<td>
<b>Building the Address Table and Address Table Changes</b>
The device dynamically builds the address table by using the MAC source address of the frames received. When the device receives a frame for a MAC destination address not listed in its address table, it floods the frame to all LAN ports of the same VLAN except the port that received the frame. When the destination station replies, the device adds its relevant MAC source address and port ID to the address table. The device then forwards subsequent frames to a single LAN port without flooding all LAN ports.

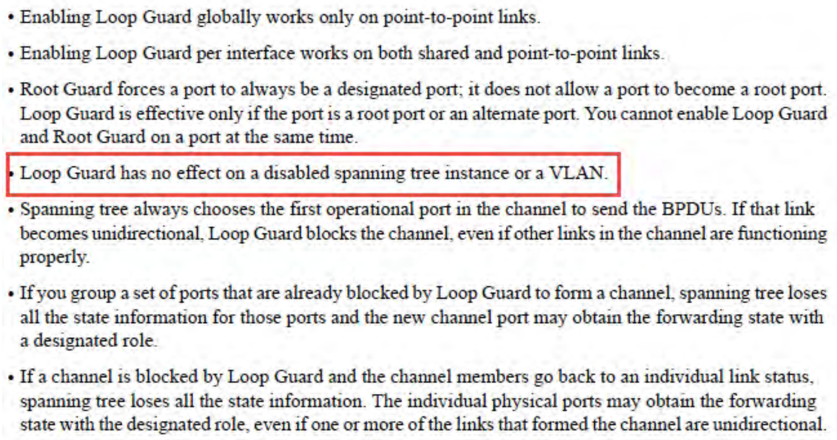
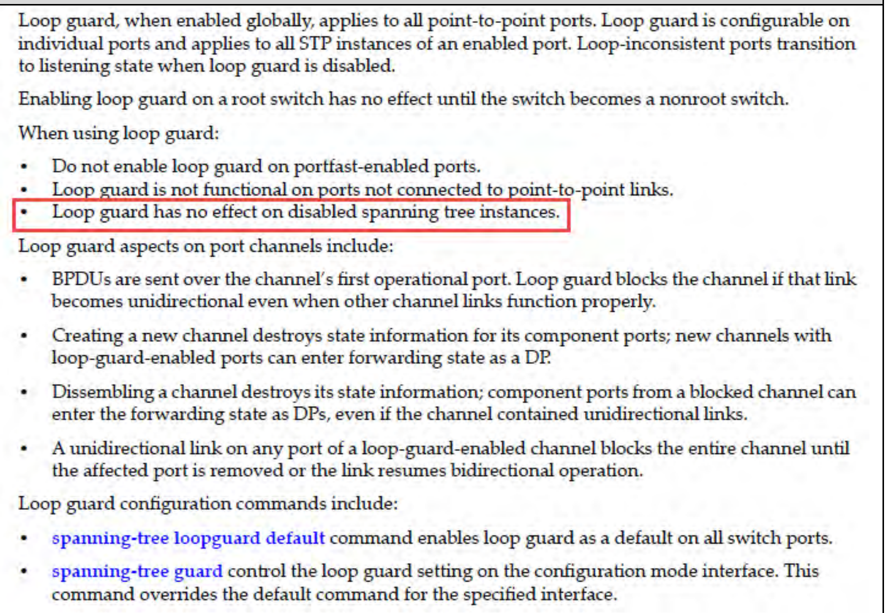
Cisco Nexus 7000 Series NX-OS Layer 2 Switching Configuration Guide (2011), at 10.</td>
<td>
<b>14.3 MAC Address Table</b>
The switch maintains an MAC address table for switching frames efficiently between ports. The MAC address table contains static and dynamic MAC addresses.
• Static MAC addresses are entered into the table through a CLI command.
• Dynamic MAC addresses are entered into the table when the switch receives a frame whose source address is not listed in the MAC address table The switch builds the table dynamically by referencing the source address of frames it receives.
When the switch receives a frame, it associates the MAC address of the transmitting interface with the recipient VLAN When a VLAN receives a frame for a MAC destination address not listed in the address table, the switch bridges the frame to all of the VLAN's ports except the recipient port. When the destination interface replies, the switch adds its MAC address to the MAC address table. The switch forwards subsequent frames with the destination address to the specified port.
A multicast address can be associated with multiple ports.

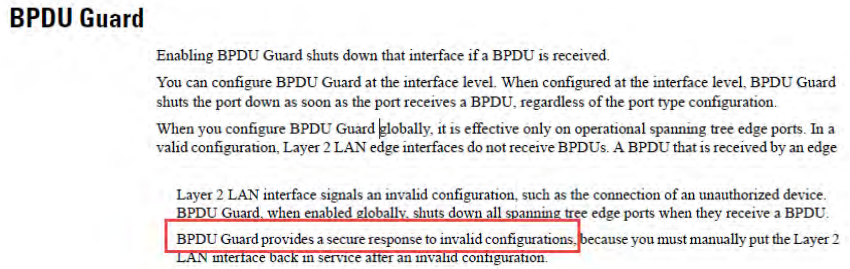
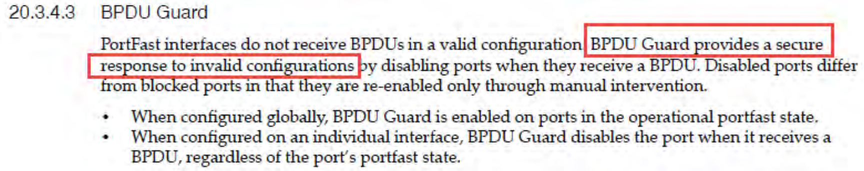
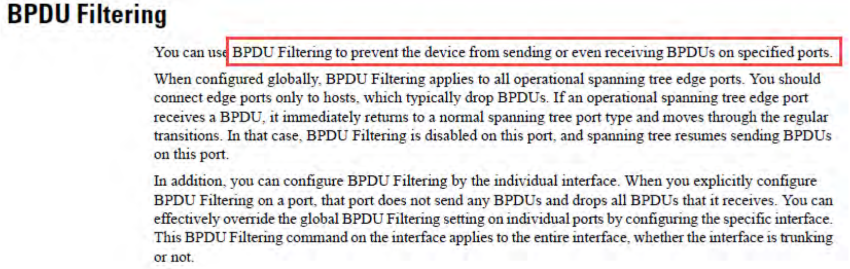
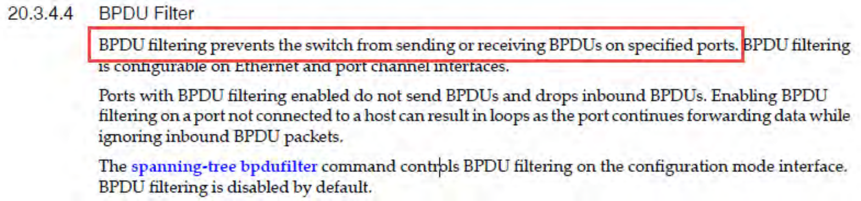
Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 624.

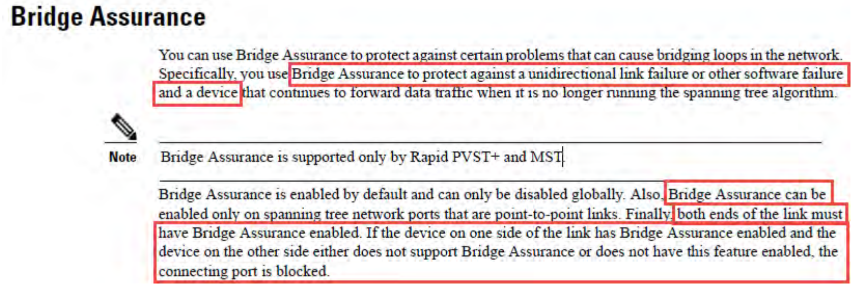
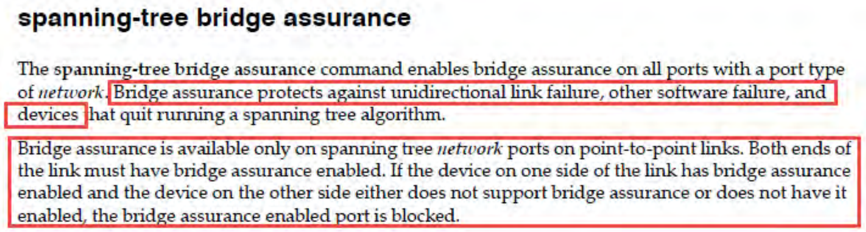
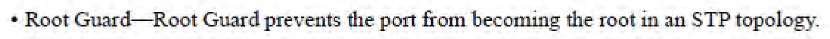
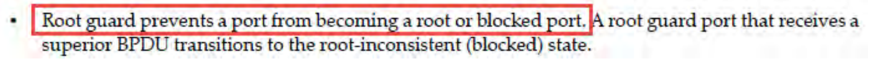
<i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 494; Arista User Manual, v. 4.11.1 (1/11/13), at 396-97; Arista User Manual v. 4.10.3 (10/22/12), at 328; Arista User Manual v. 4.9.3.2 (5/3/12), at 306.</td>
</tr>
</table>

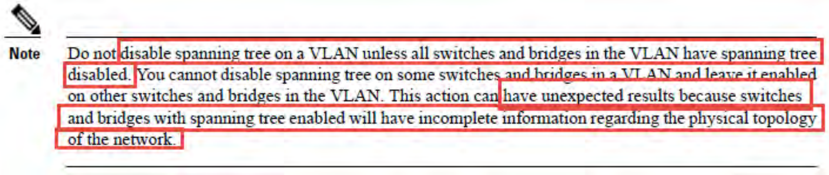
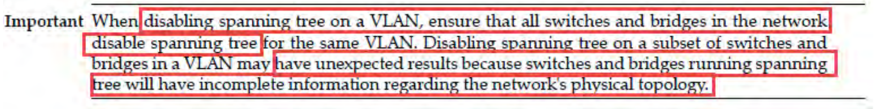
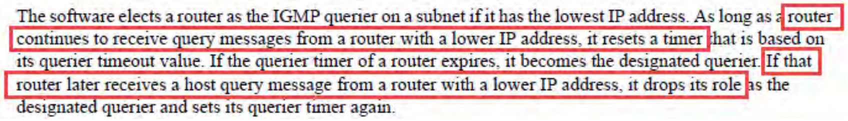
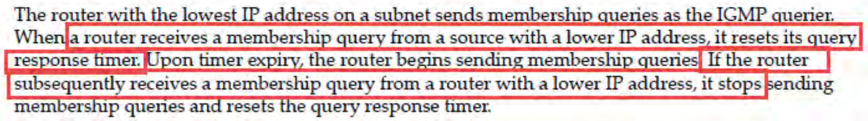
Copyright Registration Information	**Cisco**	**Arista**
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	 • Community VLAN—A community VLAN is a secondary VLAN that carries upstream traffic from the community ports to the promiscuous port gateways and to other host ports in the same community. You can configure multiple community VLANs in a private VLAN domain. The ports within one community can communicate, but these ports cannot communicate with ports in any other community or isolated VLAN in the private VLAN. Cisco Nexus 7000 Series NX-OS Layer 2 Switching Configuration Guide (2011), at 54.	 — Community Community VLAN ports carry traffic from host ports to the primary VLAN ports and to other host ports in the same community VLAN. Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 763. *See also* Arista User Manual v. 4.12.3 (7/17/13), at 611; Arista User Manual, v. 4.11.1 (1/11/13), at 467; Arista User Manual v. 4.10.3 (10/22/12), at 387; Arista User Manual v. 4.9.3.2 (5/3/12), at 307.
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	 • Protocol migration—For backward compatibility with 802.1D devices, 802.1w selectively sends 802.1D configuration BPDUs and TCN BPDUs on a per-port basis. When a port is initialized, the migrate-delay timer is started (specifies the minimum time during which 802.1w BPDUs are sent), and 802.1w BPDUs are sent. While this timer is active, the device processes all BPDUs received on that port and ignores the protocol type. If the device receives an 802.1D BPDU after the port migration-delay timer has expired, it assumes that it is connected to an 802.1D device and starts using only 802.1D BPDUs. However, if the 802.1w device is using 802.1D BPDUs on a port and receives an 802.1w BPDU after the timer has expired, it restarts the timer and starts using 802.1w BPDUs on that port. Cisco Nexus 7000 Series NX-OS Layer 2 Switching Configuration Guide (2011), at 100	 The clear spanning-tree detected-protocols command forces MST ports to renegotiate with their neighbors. RSTP provides backward compatibility with 802.1D bridges as follows: • RSTP selectively sends 802.1D-configured BPDUs and Topology Change Notification (TCN) BPDUs on a per-port basis. • When a port initializes, the migration delay timer starts and RSTP BPDUs are transmitted. While the migration delay timer is active, the bridge processes all BPDUs received on that port. • If the bridge receives an 802.1D BPDU after a port's migration delay timer expires, the bridge assumes it is connected to an 802.1D bridge and starts using only 802.1D BPDUs. • When RSTP uses 802.1D BPDUs on a port and receives an RSTP BPDU after the migration delay expires, RSTP restarts the migration delay timer and resumes using RSTP BPDUs on that port. Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 953. *See also* Arista User Manual v. 4.12.3 (7/17/13), at 831; Arista User Manual, v. 4.11.1 (1/11/13), at 649; Arista User Manual v. 4.10.3 (10/22/12), at 563; Arista User Manual v. 4.9.3.2 (5/3/12), at 483; Arista User Manual v. 4.8.2 (11/18/11), at 357; Arista User Manual v. 4.7.3 (7/18/11), at 231.

Copyright Registration Information	Cisco	Arista
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	 **Loop Guard** Loop Guard helps prevent bridging loops that could occur because of a unidirectional link failure on a point-to-point link. Cisco Nexus 7000 Series NX-OS Layer 2 Switching Configuration Guide (2011), at 176.	 • Loop Guard: Prevents loops resulting from a unidirectional link failure on a point-to-point link. Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 963. *See also* Arista User Manual v. 4.12.3 (7/17/13), at 842; Arista User Manual, v. 4.11.1 (1/11/13), at 660; Arista User Manual v. 4.10.3 (10/22/12), at 574; Arista User Manual v. 4.9.3.2 (5/3/12), at 494; Arista User Manual v. 4.8.2 (11/18/11), at 368; Arista User Manual v. 4.7.3 (7/18/11), at 242.
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	 Rapid PVST+ achieves rapid transition to the forwarding state only on edge ports and point-to-point links. Cisco Nexus 7000 Series NX-OS Layer 2 Switching Configuration Guide (2011), at 90.	 RSTP only achieves rapid transition to forwarding state on edge ports and point-to-point links. Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 964. *See also* Arista User Manual v. 4.12.3 (7/17/13), at 843; Arista User Manual, v. 4.11.1 (1/11/13), at 661; Arista User Manual v. 4.10.3 (10/22/12), at 575; Arista User Manual v. 4.9.3.2 (5/3/12), at 494; Arista User Manual v. 4.8.2 (11/18/11), at 368; Arista User Manual v. 4.7.3 (7/18/11), at 242.
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	 Enabling Loop Guard on a root device has no effect but provides protection when a root device becomes a nonroot device. Cisco Nexus 7000 Series NX-OS Layer 2 Switching Configuration Guide (2011), at 176.	 Enabling loop guard on a root switch has no effect until the switch becomes a nonroot switch. Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 966. *See also* Arista User Manual v. 4.12.3 (7/17/13), at 844; Arista User Manual, v. 4.11.1 (1/11/13), at 662; Arista User Manual v. 4.10.3 (10/22/12), at 576; Arista User Manual v. 4.9.3.2 (5/3/12), at 496; Arista User Manual v. 4.8.2 (11/18/11), at 370; Arista User Manual v. 4.7.3 (7/18/11), at 244.

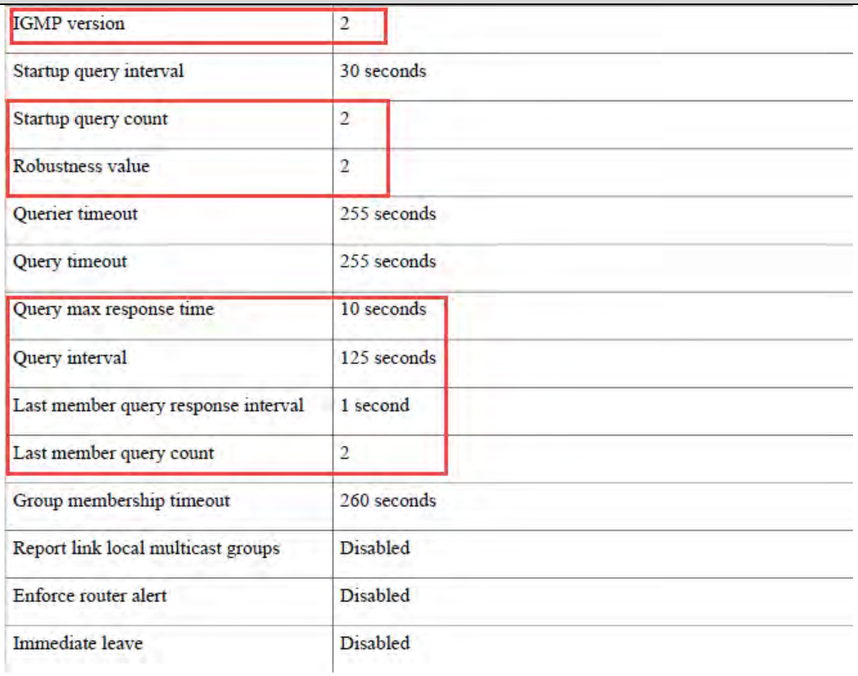
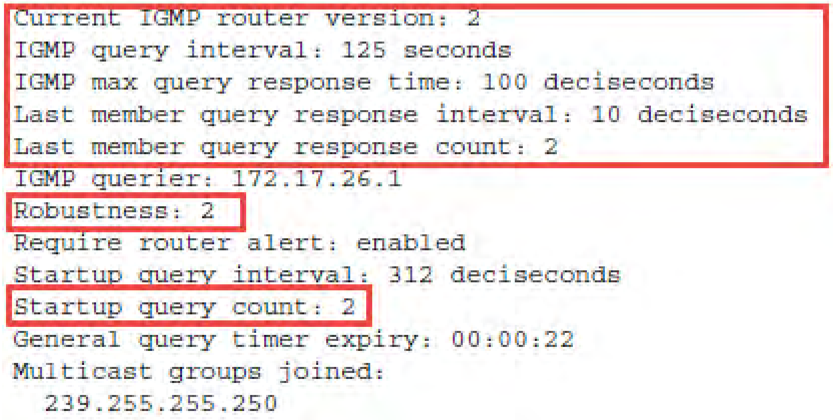
Copyright Registration Information	Cisco	Arista
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	 • Enabling Loop Guard globally works only on point-to-point links. • Enabling Loop Guard per interface works on both shared and point-to-point links. • Root Guard forces a port to always be a designated port; it does not allow a port to become a root port. Loop Guard is effective only if the port is a root port or an alternate port. You cannot enable Loop Guard and Root Guard on a port at the same time. • Loop Guard has no effect on a disabled spanning tree instance or a VLAN. • Spanning tree always chooses the first operational port in the channel to send the BPDUs. If that link becomes unidirectional, Loop Guard blocks the channel, even if other links in the channel are functioning properly. • If you group a set of ports that are already blocked by Loop Guard to form a channel, spanning tree loses all the state information for those ports and the new channel port may obtain the forwarding state with a designated role. • If a channel is blocked by Loop Guard and the channel members go back to an individual link status, spanning tree loses all the state information. The individual physical ports may obtain the forwarding state with the designated role, even if one or more of the links that formed the channel are unidirectional. Cisco Nexus 7000 Series NX-OS Layer 2 Switching Configuration Guide (2011), at 179.	 Loop guard, when enabled globally, applies to all point-to-point ports. Loop guard is configurable on individual ports and applies to all STP instances of an enabled port. Loop-inconsistent ports transition to listening state when loop guard is disabled. Enabling loop guard on a root switch has no effect until the switch becomes a nonroot switch. When using loop guard: • Do not enable loop guard on portfast-enabled ports. • Loop guard is not functional on ports not connected to point-to-point links. • Loop guard has no effect on disabled spanning tree instances. Loop guard aspects on port channels include: • BPDUs are sent over the channel's first operational port. Loop guard blocks the channel if that link becomes unidirectional even when other channel links function properly. • Creating a new channel destroys state information for its component ports; new channels with loop-guard-enabled ports can enter forwarding state as a DP. • Dissembling a channel destroys its state information; component ports from a blocked channel can enter the forwarding state as DPs, even if the channel contained unidirectional links. • A unidirectional link on any port of a loop-guard-enabled channel blocks the entire channel until the affected port is removed or the link resumes bidirectional operation. Loop guard configuration commands include: • spanning-tree loopguard default command enables loop guard as a default on all switch ports. • spanning-tree guard control the loop guard setting on the configuration mode interface. This command overrides the default command for the specified interface. Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 966. *See also* Arista User Manual v. 4.12.3 (7/17/13), at 844; Arista User Manual, v. 4.11.1 (1/11/13), at 662; Arista User Manual v. 4.10.3 (10/22/12), at 576; Arista User Manual v. 4.9.3.2 (5/3/12), at 496; Arista User Manual v. 4.8.2 (11/18/11), at 370; Arista User Manual v. 4.7.3 (7/18/11), at 245.

Copyright Registration Information	Cisco	Arista
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	 **BPDU Guard** Enabling BPDU Guard shuts down that interface if a BPDU is received. You can configure BPDU Guard at the interface level. When configured at the interface level, BPDU Guard shuts the port down as soon as the port receives a BPDU, regardless of the port type configuration. When you configure BPDU Guard globally, it is effective only on operational spanning tree edge ports. In a valid configuration, Layer 2 LAN edge interfaces do not receive BPDUs. A BPDU that is received by an edge Layer 2 LAN interface signals an invalid configuration, such as the connection of an unauthorized device. BPDU Guard, when enabled globally, shuts down all spanning tree edge ports when they receive a BPDU. BPDU Guard provides a secure response to invalid configurations, because you must manually put the Layer 2 LAN interface back in service after an invalid configuration. Cisco Nexus 7000 Series NX-OS Layer 2 Switching Configuration Guide (2011), at 174-75.	 20.3.4.3 BPDU Guard PortFast interfaces do not receive BPDUs in a valid configuration BPDU Guard provides a secure response to invalid configurations by disabling ports when they receive a BPDU. Disabled ports differ from blocked ports in that they are re-enabled only through manual intervention. • When configured globally, BPDU Guard is enabled on ports in the operational portfast state. • When configured on an individual interface, BPDU Guard disables the port when it receives a BPDU, regardless of the port's portfast state. Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 968. *See also* Arista User Manual v. 4.12.3 (7/17/13), at 846; Arista User Manual, v. 4.11.1 (1/11/13), at 664-65; Arista User Manual v. 4.10.3 (10/22/12), at 578; Arista User Manual v. 4.9.3.2 (5/3/12), at 498; Arista User Manual v. 4.8.2 (11/18/11), at 372; Arista User Manual v. 4.7.3 (7/18/11), at 246.
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	 **BPDU Filtering** You can use BPDU Filtering to prevent the device from sending or even receiving BPDUs on specified ports. When configured globally, BPDU Filtering applies to all operational spanning tree edge ports. You should connect edge ports only to hosts, which typically drop BPDUs. If an operational spanning tree edge port receives a BPDU, it immediately returns to a normal spanning tree port type and moves through the regular transitions. In that case, BPDU Filtering is disabled on this port, and spanning tree resumes sending BPDUs on this port. In addition, you can configure BPDU Filtering by the individual interface. When you explicitly configure BPDU Filtering on a port, that port does not send any BPDUs and drops all BPDUs that it receives. You can effectively override the global BPDU Filtering setting on individual ports by configuring the specific interface. This BPDU Filtering command on the interface applies to the entire interface, whether the interface is trunking or not. Cisco Nexus 7000 Series NX-OS Layer 2 Switching Configuration Guide (2011), at 175.	 20.3.4.4 BPDU Filter BPDU filtering prevents the switch from sending or receiving BPDUs on specified ports. BPDU filtering is configurable on Ethernet and port channel interfaces. Ports with BPDU filtering enabled do not send BPDUs and drops inbound BPDUs. Enabling BPDU filtering on a port not connected to a host can result in loops as the port continues forwarding data while ignoring inbound BPDU packets. The spanning-tree bpdufilter command controls BPDU filtering on the configuration mode interface. BPDU filtering is disabled by default. Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 968. *See also* Arista User Manual v. 4.12.3 (7/17/13), at 846-47; Arista User Manual, v. 4.11.1 (1/11/13), at 665; Arista User Manual v. 4.10.3 (10/22/12), at 579; Arista User Manual v. 4.9.3.2 (5/3/12), at 498; Arista User Manual v. 4.8.2 (11/18/11), at 372; Arista User Manual v. 4.7.3 (7/18/11), at 246.

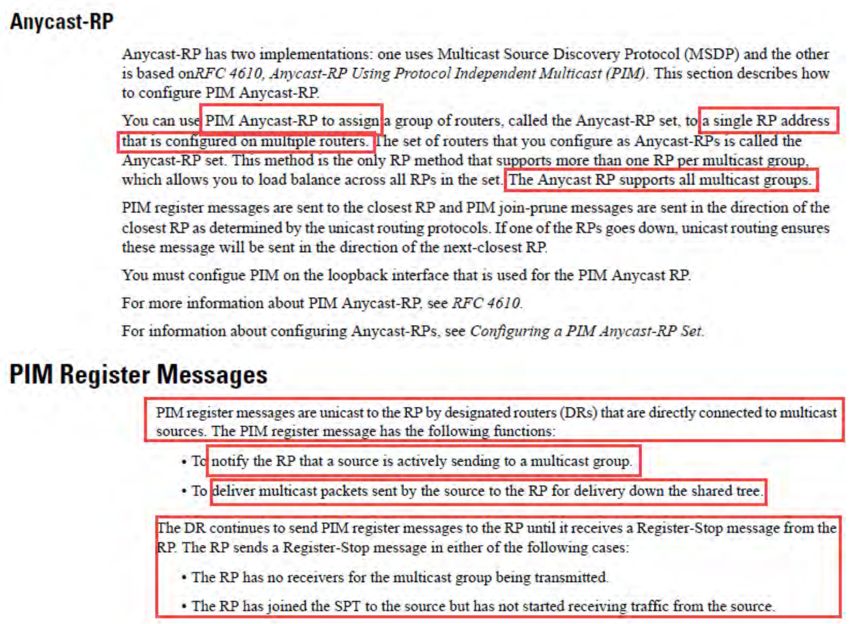
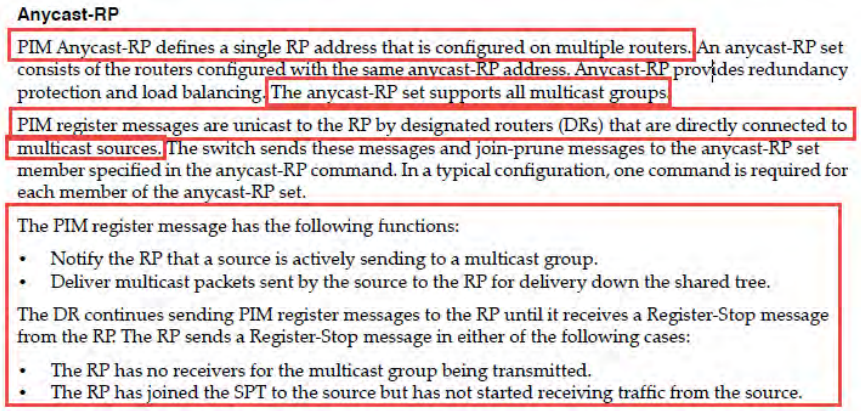
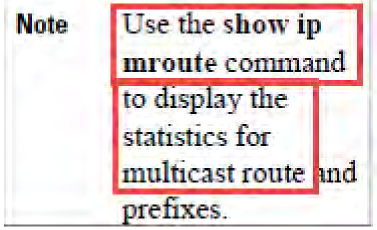
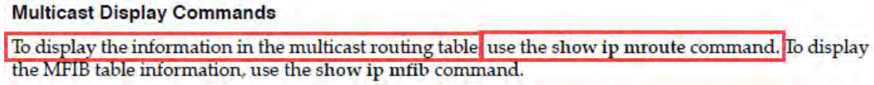
Copyright Registration Information	Cisco	Arista
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	 **Bridge Assurance** You can use Bridge Assurance to protect against certain problems that can cause bridging loops in the network. Specifically, you use Bridge Assurance to protect against a unidirectional link failure or other software failure and a device that continues to forward data traffic when it is no longer running the spanning tree algorithm. Note Bridge Assurance is supported only by Rapid PVST+ and MST. Bridge Assurance is enabled by default and can only be disabled globally. Also, Bridge Assurance can be enabled only on spanning tree network ports that are point-to-point links. Finally, both ends of the link must have Bridge Assurance enabled. If the device on one side of the link has Bridge Assurance enabled and the device on the other side either does not support Bridge Assurance or does not have this feature enabled, the connecting port is blocked. Cisco Nexus 7000 Series NX-OS Layer 2 Switching Configuration Guide (2011), at 175.	 **spanning-tree bridge assurance** The spanning-tree bridge assurance command enables bridge assurance on all ports with a port type of *network*. Bridge assurance protects against unidirectional link failure, other software failure, and devices hat quit running a spanning tree algorithm. Bridge assurance is available only on spanning tree *network* ports on point-to-point links. Both ends of the link must have bridge assurance enabled. If the device on one side of the link has bridge assurance enabled and the device on the other side either does not support bridge assurance or does not have it enabled, the bridge assurance enabled port is blocked. Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 1002. *See also* Arista User Manual v. 4.12.3 (7/17/13), at 880; Arista User Manual, v. 4.11.1 (1/11/13), at 698; Arista User Manual v. 4.10.3 (10/22/12), at 612; Arista User Manual v. 4.9.3.2 (5/3/12), at 531; Arista User Manual v. 4.8.2 (11/18/11), at 403; Arista User Manual v. 4.7.3 (7/18/11), at 252.
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	 • Root Guard—Root Guard prevents the port from becoming the root in an STP topology. Cisco Nexus 7000 Series NX-OS Layer 2 Switching Configuration Guide (2011), at 6.	 • Root guard prevents a port from becoming a root or blocked port. A root guard port that receives a superior BPDU transitions to the root-inconsistent (blocked) state. Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 1005. *See also* Arista User Manual v. 4.12.3 (7/17/13), at 883; Arista User Manual, v. 4.11.1 (1/11/13), at 701; Arista User Manual v. 4.10.3 (10/22/12), at 615; Arista User Manual v. 4.9.3.2 (5/3/12), at 534; Arista User Manual v. 4.8.2 (11/18/11), at 406; Arista User Manual v. 4.7.3 (7/18/11), at 268.

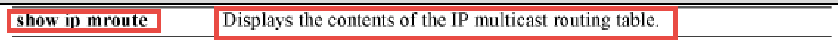
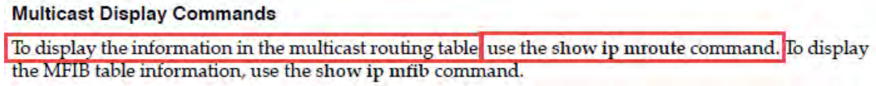
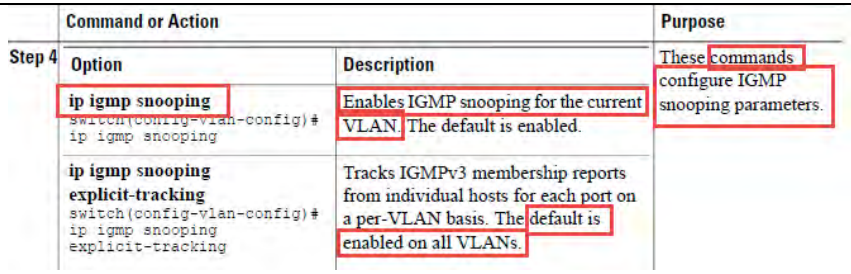
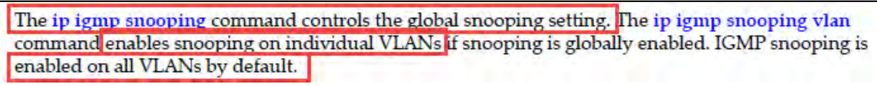
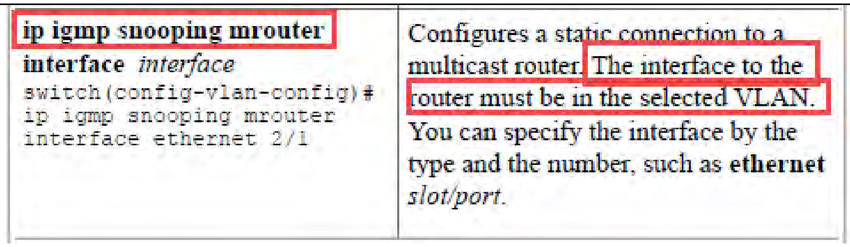
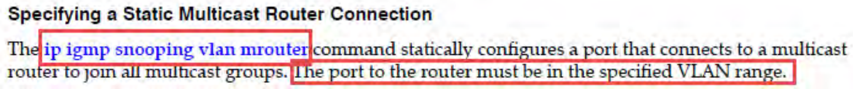
Copyright Registration Information	Cisco	Arista
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	 Note Do not disable spanning tree on a VLAN unless all switches and bridges in the VLAN have spanning tree disabled. You cannot disable spanning tree on some switches and bridges in a VLAN and leave it enabled on other switches and bridges in the VLAN. This action can have unexpected results because switches and bridges with spanning tree enabled will have incomplete information regarding the physical topology of the network. Cisco Nexus 7000 Series NX-OS Layer 2 Switching Configuration Guide (2011), at 108.	 Important When disabling spanning tree on a VLAN, ensure that all switches and bridges in the network disable spanning tree for the same VLAN. Disabling spanning tree on a subset of switches and bridges in a VLAN may have unexpected results because switches and bridges running spanning tree will have incomplete information regarding the network's physical topology. Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 1023. *See also* Arista User Manual v. 4.12.3 (7/17/13), at 901; Arista User Manual, v. 4.11.1 (1/11/13), at 719; Arista User Manual v. 4.10.3 (10/22/12), at 633; Arista User Manual v. 4.9.3.2 (5/3/12), at 550; Arista User Manual v. 4.8.2 (11/18/11), at 422; Arista User Manual v. 4.7.3 (7/18/11), at 264.
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	 The software elects a router as the IGMP querier on a subnet if it has the lowest IP address. As long as a router continues to receive query messages from a router with a lower IP address, it resets a timer that is based on its querier timeout value. If the querier timer of a router expires, it becomes the designated querier. If that router later receives a host query message from a router with a lower IP address, it drops its role as the designated querier and sets its querier timer again. Cisco Nexus 7000 Series NX-OS Multicast Routing Configuration Guide (2012), at 20 .	 The router with the lowest IP address on a subnet sends membership queries as the IGMP querier. When a router receives a membership query from a source with a lower IP address, it resets its query response timer. Upon timer expiry, the router begins sending membership queries. If the router subsequently receives a membership query from a router with a lower IP address, it stops sending membership queries and resets the query response timer. Arista User Manual v. 4v. 4.14.3F - Rev. 2 (10/2/14), at 1779. *See also* Arista User Manual v. 4.12.3 (7/17/13), at 1505; Arista User Manual, v. 4.11.1 (1/11/13), at 1205; Arista User Manual v. 4.10.3 (10/22/12), at 999; Arista User Manual v. 4.9.3.2 (5/3/12), at 757; Arista User Manual v. 4.8.2 (11/18/11), at 579; Arista User Manual v. 4.7.3 (7/18/11), at 459; Arista User Manual v. 4.6.0 (12/22/2010), at 309

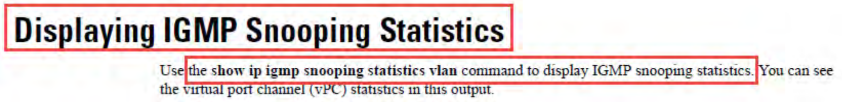
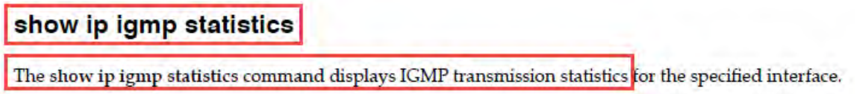
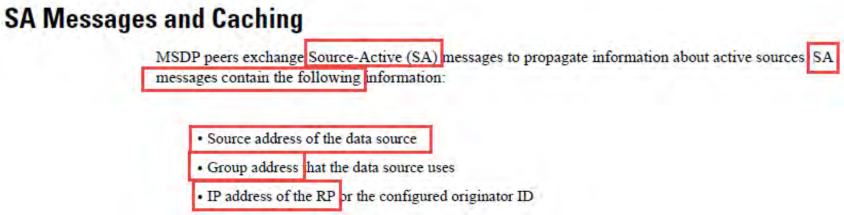
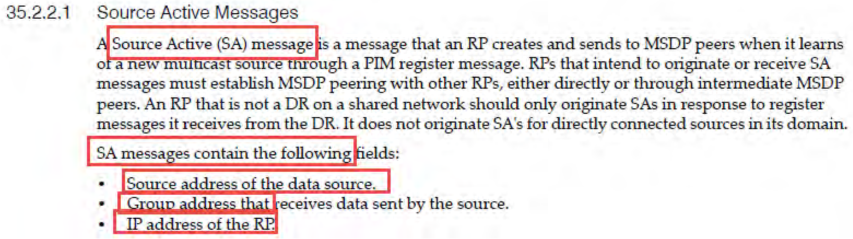
<table>
<tr><th>Copyright Registration Information</th><th>Cisco</th><th>Arista</th></tr>
<tr>
<td>Cisco NX-OS 6.2

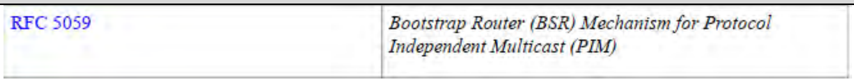
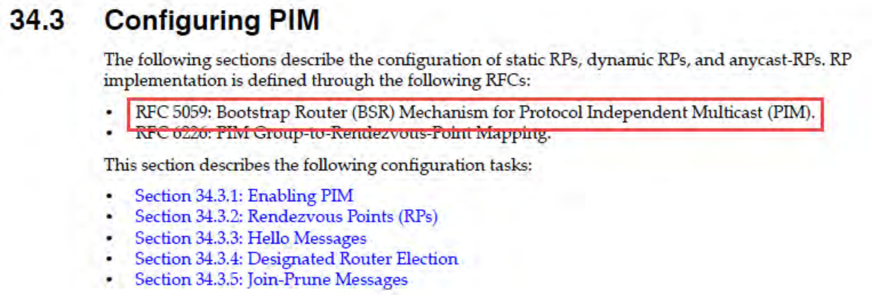
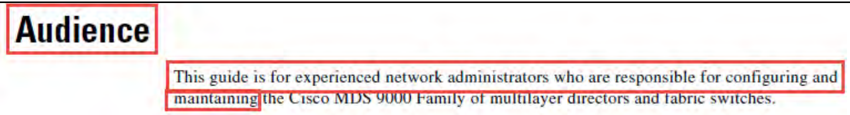
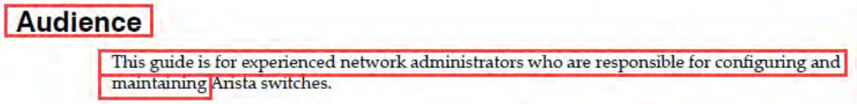
Effective date of registration: 11/13/2014</td>
<td>
<table>
<tr><td>IGMP version</td><td>2</td></tr>
<tr><td>Startup query interval</td><td>30 seconds</td></tr>
<tr><td>Startup query count</td><td>2</td></tr>
<tr><td>Robustness value</td><td>2</td></tr>
<tr><td>Querier timeout</td><td>255 seconds</td></tr>
<tr><td>Query timeout</td><td>255 seconds</td></tr>
<tr><td>Query max response time</td><td>10 seconds</td></tr>
<tr><td>Query interval</td><td>125 seconds</td></tr>
<tr><td>Last member query response interval</td><td>1 second</td></tr>
<tr><td>Last member query count</td><td>2</td></tr>
<tr><td>Group membership timeout</td><td>260 seconds</td></tr>
<tr><td>Report link local multicast groups</td><td>Disabled</td></tr>
<tr><td>Enforce router alert</td><td>Disabled</td></tr>
<tr><td>Immediate leave</td><td>Disabled</td></tr>
</table>
Cisco Nexus 7000 Series NX-OS Multicast Routing Configuration Guide (2012), at 24.</td>
<td>
<pre>
Current IGMP router version: 2
IGMP query interval: 125 seconds
IGMP max query response time: 100 deciseconds
Last member query response interval: 10 deciseconds
Last member query response count: 2
IGMP querier: 172.17.26.1
Robustness: 2
Require router alert: enabled
Startup query interval: 312 deciseconds
Startup query count: 2
General query timer expiry: 00:00:22
Multicast groups joined:
  239.255.255.250
</pre>
Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 1850.

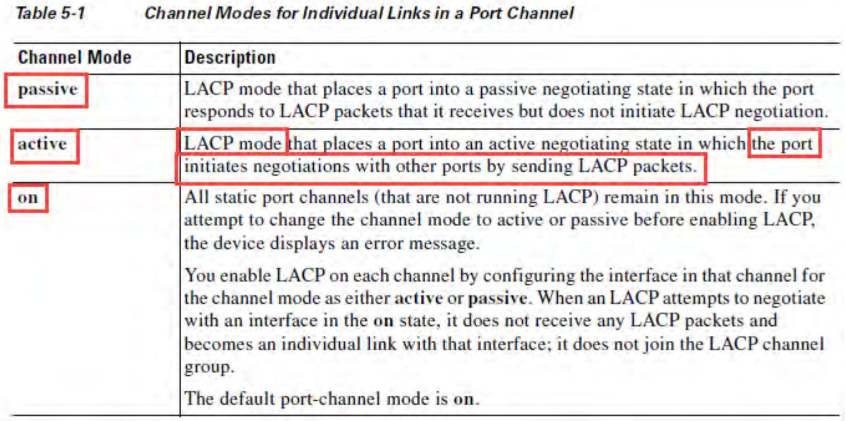
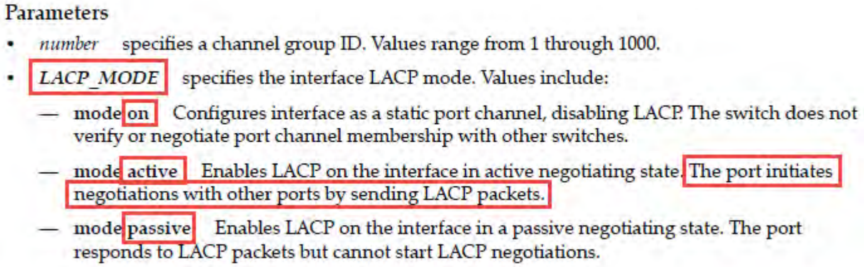
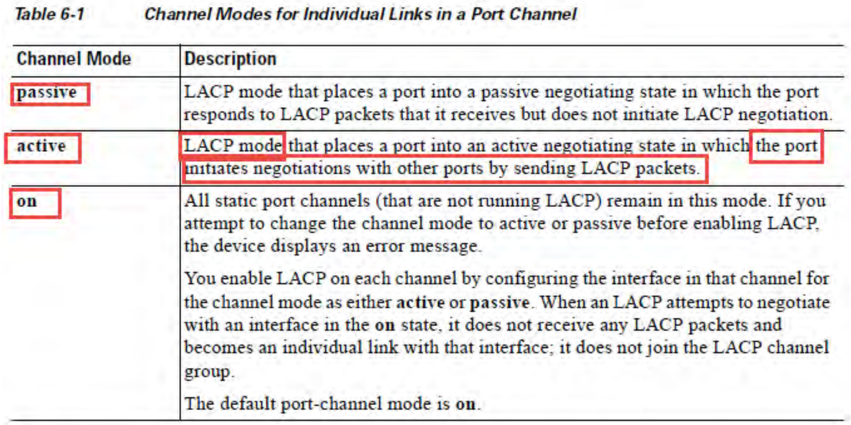
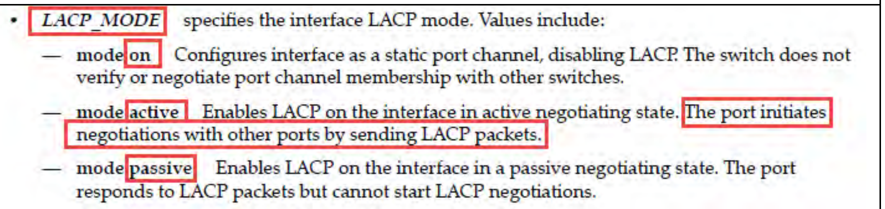
<i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 1558; Arista User Manual, v. 4.11.1 (1/11/13), at 1253; Arista User Manual v. 4.10.3 (10/22/12), at 1038; Arista User Manual v. 4.9.3.2 (5/3/12), at 796; Arista User Manual v. 4.8.2 (11/18/11), at 614; Arista User Manual v. 4.7.3 (7/18/11), at 491; Arista User Manual v. 4.6.0 (12/22/2010), at 337.</td>
</tr>
</table>

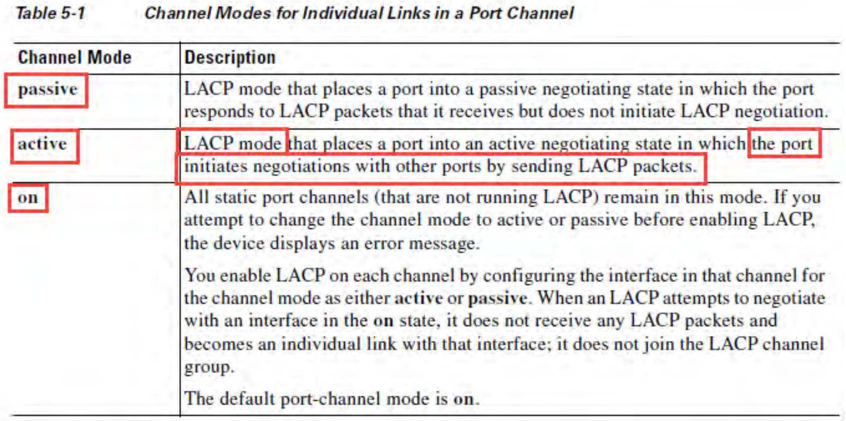
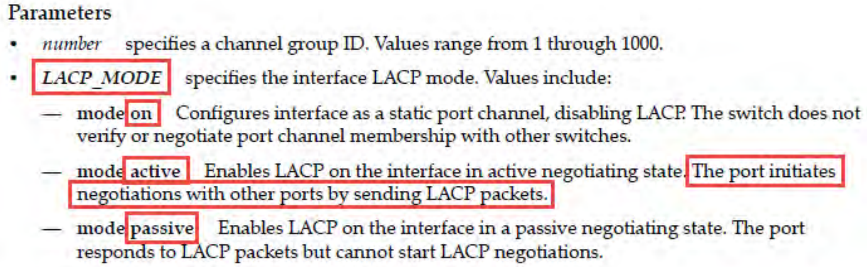
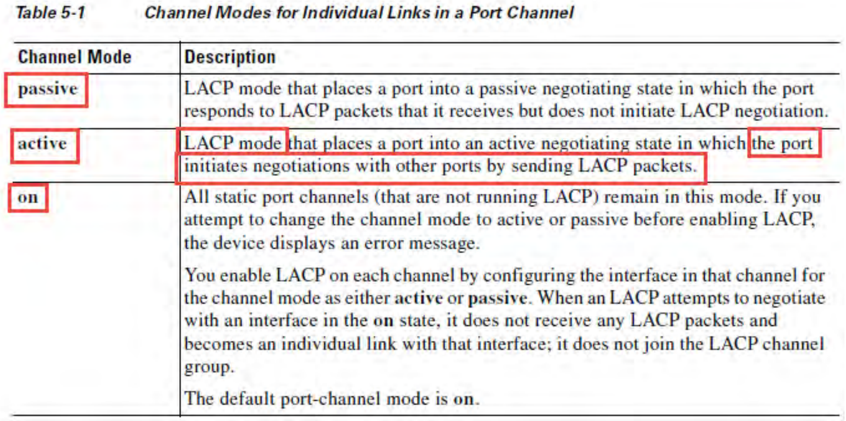
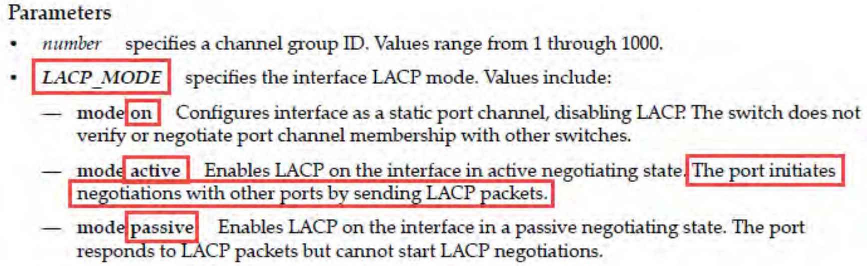
Copyright Registration Information	Cisco	Arista
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	 **Anycast-RP** Anycast-RP has two implementations: one uses Multicast Source Discovery Protocol (MSDP) and the other is based onRFC 4610, *Anycast-RP Using Protocol Independent Multicast (PIM)*. This section describes how to configure PIM Anycast-RP. You can use PIM Anycast-RP to assign a group of routers, called the Anycast-RP set, to a single RP address that is configured on multiple routers. The set of routers that you configure as Anycast-RPs is called the Anycast-RP set. This method is the only RP method that supports more than one RP per multicast group, which allows you to load balance across all RPs in the set. The Anycast RP supports all multicast groups. PIM register messages are sent to the closest RP and PIM join-prune messages are sent in the direction of the closest RP as determined by the unicast routing protocols. If one of the RPs goes down, unicast routing ensures these message will be sent in the direction of the next-closest RP. You must configue PIM on the loopback interface that is used for the PIM Anycast RP. For more information about PIM Anycast-RP, see *RFC 4610*. For information about configuring Anycast-RPs, see *Configuring a PIM Anycast-RP Set*. **PIM Register Messages** PIM register messages are unicast to the RP by designated routers (DRs) that are directly connected to multicast sources. The PIM register message has the following functions: • To notify the RP that a source is actively sending to a multicast group. • To deliver multicast packets sent by the source to the RP for delivery down the shared tree. The DR continues to send PIM register messages to the RP until it receives a Register-Stop message from the RP. The RP sends a Register-Stop message in either of the following cases: • The RP has no receivers for the multicast group being transmitted. • The RP has joined the SPT to the source but has not started receiving traffic from the source. Cisco Nexus 7000 Series NX-OS Multicast Routing Configuration Guide (2012), at 68-69.	 **Anycast-RP** PIM Anycast-RP defines a single RP address that is configured on multiple routers. An anycast-RP set consists of the routers configured with the same anycast-RP address. Anycast-RP provides redundancy protection and load balancing. The anycast-RP set supports all multicast groups. PIM register messages are unicast to the RP by designated routers (DRs) that are directly connected to multicast sources. The switch sends these messages and join-prune messages to the anycast-RP set member specified in the anycast-RP command. In a typical configuration, one command is required for each member of the anycast-RP set. The PIM register message has the following functions: • Notify the RP that a source is actively sending to a multicast group. • Deliver multicast packets sent by the source to the RP for delivery down the shared tree. The DR continues sending PIM register messages to the RP until it receives a Register-Stop message from the RP. The RP sends a Register-Stop message in either of the following cases: • The RP has no receivers for the multicast group being transmitted. • The RP has joined the SPT to the source but has not started receiving traffic from the source. Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 1874. *See also* Arista User Manual v. 4.12.3 (7/17/13), at 1580; Arista User Manual, v. 4.11.1 (1/11/13), at 1274; Arista User Manual v. 4.10.3 (10/22/12), at 1005-06; Arista User Manual v. 4.9.3.2 (5/3/12), at 763-64; Arista User Manual v. 4.8.2 (11/18/11), at 639; Arista User Manual v. 4.7.3 (7/18/11), at 514.
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	 **Note** Use the show ip mroute command to display the statistics for multicast route and prefixes. Cisco Nexus 7000 Series NX-OS Multicast Routing Configuration Guide (2012), at 118 .	 **Multicast Display Commands** To display the information in the multicast routing table use the show ip mroute command. To display the MFIB table information, use the show ip mfib command. Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 1758. *See also* Arista User Manual v. 4.12.3 (7/17/13), at 1486; Arista User Manual, v. 4.11.1 (1/11/13), at 1188; Arista User Manual v. 4.10.3 (10/22/12), at 1012; Arista User Manual v. 4.9.3.2 (5/3/12), at 770; Arista User Manual v. 4.8.2 (11/18/11), at 589; Arista User Manual v. 4.7.3 (7/18/11), at 469; Arista User Manual v. 4.6.0 (12/22/2010), at 319.

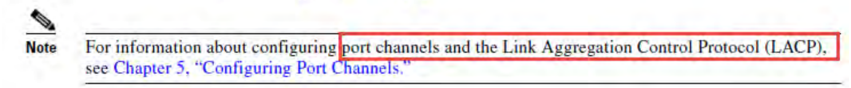
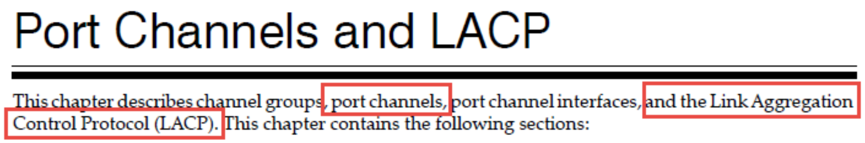
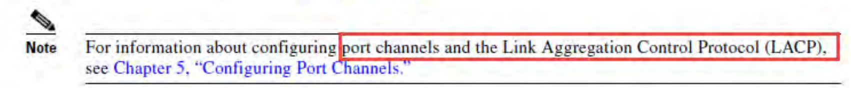
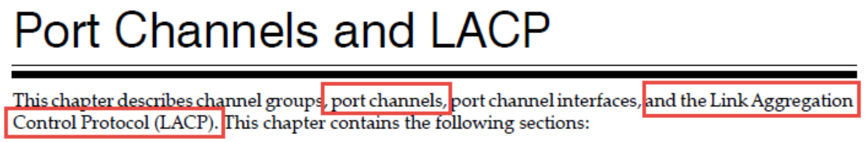
Copyright Registration Information	Cisco	Arista
Cisco IOS 12.4 Effective date of registration: 8/12/2005	 show ip mroute — Displays the contents of the IP multicast routing table. Cisco IOS IP Multicast Command Reference (July 16, 2005), at 12.	 **Multicast Display Commands** To display the information in the multicast routing table use the show ip mroute command. To display the MFIB table information, use the show ip mfib command. Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 1758 *See also* Arista User Manual v. 4.12.3 (7/17/13), at 1486; Arista User Manual, v. 4.11.1 (1/11/13), at 1188; Arista User Manual v. 4.10.3 (10/22/12), at 1012; Arista User Manual v. 4.9.3.2 (5/3/12), at 770; Arista User Manual v. 4.8.2 (11/18/11), at 589; Arista User Manual v. 4.7.3 (7/18/11), at 469; Arista User Manual v. 4.6.0 (12/22/2010), at 319
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	 **Command or Action** / **Purpose** **Step 4** — **Option** / **Description** **ip igmp snooping** `switch(config-vlan-config)# ip igmp snooping` — Enables IGMP snooping for the current VLAN. The default is enabled. **ip igmp snooping explicit-tracking** `switch(config-vlan-config)# ip igmp snooping explicit-tracking` — Tracks IGMPv3 membership reports from individual hosts for each port on a per-VLAN basis. The default is enabled on all VLANs. Purpose: These commands configure IGMP snooping parameters. Cisco Nexus 7000 Series NX-OS Multicast Routing Configuration Guide (2012), at 139	 The ip igmp snooping command controls the global snooping setting. The ip igmp snooping vlan command enables snooping on individual VLANs if snooping is globally enabled. IGMP snooping is enabled on all VLANs by default. Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 1780 *See also* Arista User Manual v. 4.12.3 (7/17/13), at 1506; Arista User Manual, v. 4.11.1 (1/11/13), at 1206; Arista User Manual v. 4.10.3 (10/22/12), at 998; Arista User Manual v. 4.9.3.2 (5/3/12), at 756; Arista User Manual v. 4.8.2 (11/18/11), at 581; Arista User Manual v. 4.7.3 (7/18/11), at 461.
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	 **ip igmp snooping mrouter interface** *interface* `switch(config-vlan-config)# ip igmp snooping mrouter interface ethernet 2/1` — Configures a static connection to a multicast router. The interface to the router must be in the selected VLAN. You can specify the interface by the type and the number, such as **ethernet** *slot/port*. Cisco Nexus 7000 Series NX-OS Multicast Routing Configuration Guide (2012), at 140.	 **Specifying a Static Multicast Router Connection** The ip igmp snooping vlan mrouter command statically configures a port that connects to a multicast router to join all multicast groups. The port to the router must be in the specified VLAN range. Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 1780 *See also* Arista User Manual v. 4.12.3 (7/17/13), at 1506; Arista User Manual, v. 4.11.1 (1/11/13), at 1206; Arista User Manual v. 4.10.3 (10/22/12), at 1003; Arista User Manual v. 4.9.3.2 (5/3/12), at 761; Arista User Manual v. 4.8.2 (11/18/11), at 584; Arista User Manual v. 4.7.3 (7/18/11), at 503; Arista User Manual v. 4.6.0 (12/22/2010), at 349.

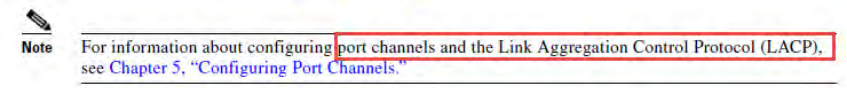
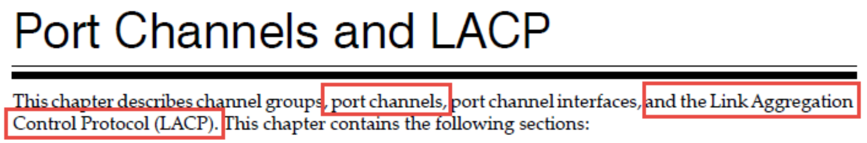
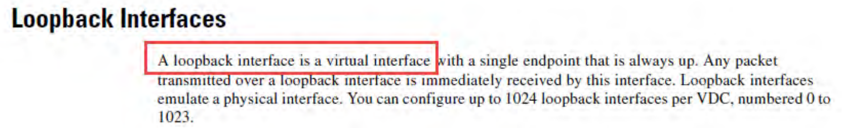
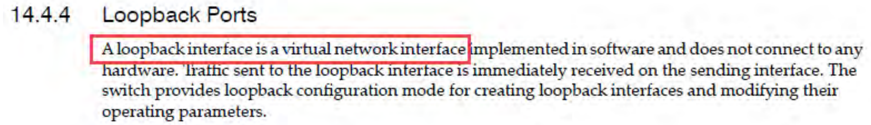
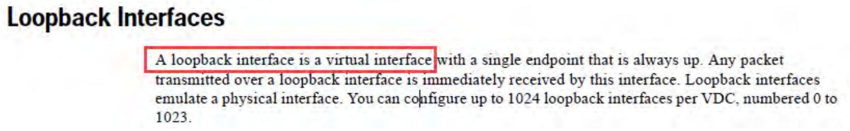
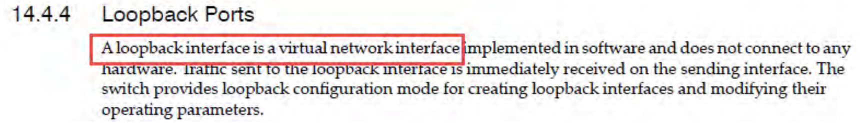
Copyright Registration Information	Cisco	Arista
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	 **Displaying IGMP Snooping Statistics** Use the **show ip igmp snooping statistics vlan** command to display IGMP snooping statistics. You can see the virtual port channel (vPC) statistics in this output. Cisco Nexus 7000 Series NX-OS Multicast Routing Configuration Guide (2012), at 144	 **show ip igmp statistics** The show ip igmp statistics command displays IGMP transmission statistics for the specified interface. Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 1867.
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	 **SA Messages and Caching** MSDP peers exchange Source-Active (SA) messages to propagate information about active sources. SA messages contain the following information: • Source address of the data source • Group address that the data source uses • IP address of the RP or the configured originator ID Cisco Nexus 7000 Series NX-OS Multicast Routing Configuration Guide (2012), at 148-49	 35.2.2.1 Source Active Messages A Source Active (SA) message is a message that an RP creates and sends to MSDP peers when it learns of a new multicast source through a PIM register message. RPs that intend to originate or receive SA messages must establish MSDP peering with other RPs, either directly or through intermediate MSDP peers. An RP that is not a DR on a shared network should only originate SAs in response to register messages it receives from the DR. It does not originate SA's for directly connected sources in its domain. SA messages contain the following fields: • Source address of the data source. • Group address that receives data sent by the source. • IP address of the RP. Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 1912. Arista User Manual v. 4.12.3 (7/17/13), at 1618; Arista User Manual, v. 4.11.1 (1/11/13), at 1310.

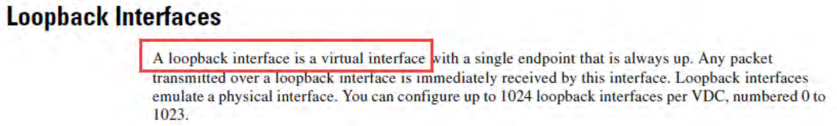
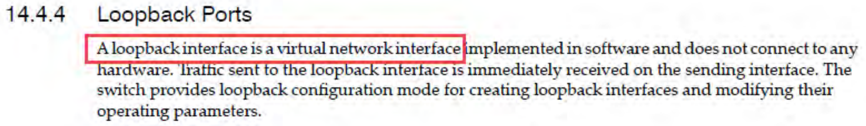
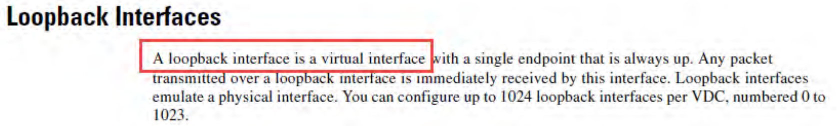
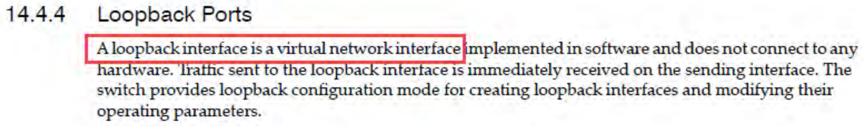
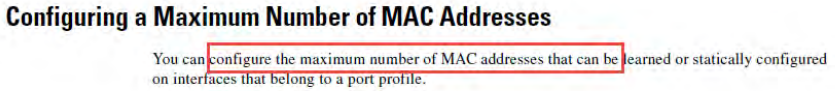
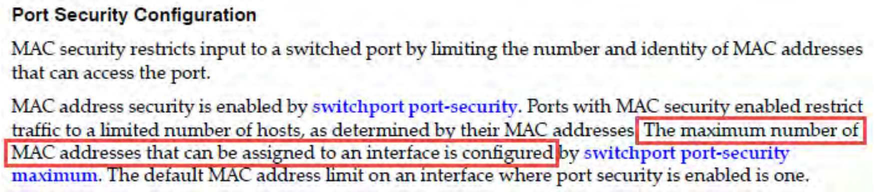
Copyright Registration Information	Cisco	Arista
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	 RFC 5059 | *Bootstrap Router (BSR) Mechanism for Protocol Independent Multicast (PIM)* Cisco Nexus 7000 Series NX-OS Multicast Routing Configuration Guide (2012), at 174.	 34.3 Configuring PIM The following sections describe the configuration of static RPs, dynamic RPs, and anycast-RPs. RP implementation is defined through the following RFCs: • RFC 5059: Bootstrap Router (BSR) Mechanism for Protocol Independent Multicast (PIM). • RFC 6226: PIM Group-to-Rendezvous-Point Mapping. This section describes the following configuration tasks: • Section 34.3.1: Enabling PIM • Section 34.3.2: Rendezvous Points (RPs) • Section 34.3.3: Hello Messages • Section 34.3.4: Designated Router Election • Section 34.3.5: Join-Prune Messages Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 1872. *See also* Arista User Manual v. 4.12.3 (7/17/13), at 1578; Arista User Manual, v. 4.11.1 (1/11/13), at 1272; Arista User Manual v. 4.10.3 (10/22/12), at 1004; Arista User Manual v. 4.9.3.2 (5/3/12), at 762.
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	 Audience This guide is for experienced network administrators who are responsible for configuring and maintaining the Cisco MDS 9000 Family of multilayer directors and fabric switches. Cisco DCNM Fundamentals Guide, Release 6.x (2011), at lxi.	 Audience This guide is for experienced network administrators who are responsible for configuring and maintaining Arista switches. Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 41. *See also* Arista User Manual v. 4.12.3 (7/17/13), at 35; Arista User Manual, v. 4.11.1 (1/11/13), at 29; Arista User Manual v. 4.10.3 (10/22/12), at 27; Arista User Manual v. 4.9.3.2 (5/3/12), at 23; Arista User Manual v. 4.8.2 (11/18/11), at 19; Arista User Manual v. 4.7.3 (7/18/11), at 17; Arista User Manual v. 4.6.0 (12/22/2010), at 13

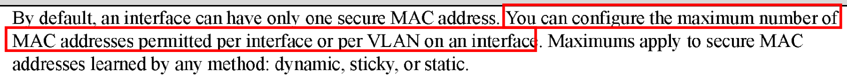
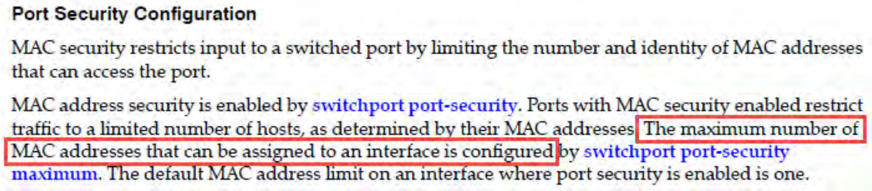
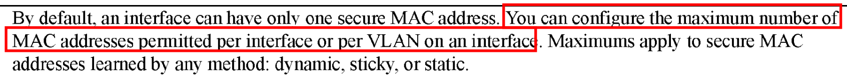
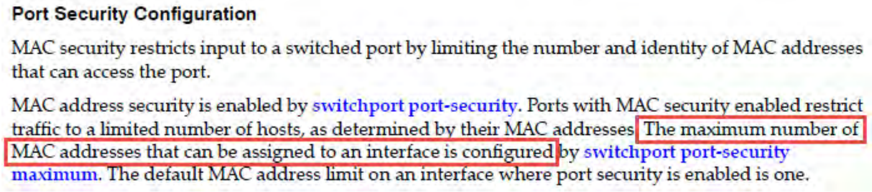
<table>
<tr><th>Copyright Registration Information</th><th>Cisco</th><th>Arista</th></tr>
<tr>
<td>Cisco NX-OS 6.2
Effective date of registration: 11/13/2014</td>
<td>

<i>Table 5-1 Channel Modes for Individual Links in a Port Channel</i>
<table>
<tr><th>Channel Mode</th><th>Description</th></tr>
<tr><td>passive</td><td>LACP mode that places a port into a passive negotiating state in which the port responds to LACP packets that it receives but does not initiate LACP negotiation.</td></tr>
<tr><td>active</td><td>LACP mode that places a port into an active negotiating state in which the port initiates negotiations with other ports by sending LACP packets.</td></tr>
<tr><td>on</td><td>All static port channels (that are not running LACP) remain in this mode. If you attempt to change the channel mode to active or passive before enabling LACP, the device displays an error message.
You enable LACP on each channel by configuring the interface in that channel for the channel mode as either <b>active</b> or <b>passive</b>. When an LACP attempts to negotiate with an interface in the <b>on</b> state, it does not receive any LACP packets and becomes an individual link with that interface; it does not join the LACP channel group.
The default port-channel mode is <b>on</b>.</td></tr>
</table>
Interfaces Configuration Guide, Cisco DCNM for LAN, Release 6.x (2012), at 5-10
</td>
<td>

Parameters
<ul>
<li><i>number</i> specifies a channel group ID. Values range from 1 through 1000.</li>
<li><i>LACP_MODE</i> specifies the interface LACP mode. Values include:
<ul>
<li>— mode on Configures interface as a static port channel, disabling LACP. The switch does not verify or negotiate port channel membership with other switches.</li>
<li>— mode active Enables LACP on the interface in active negotiating state. The port initiates negotiations with other ports by sending LACP packets.</li>
<li>— mode passive Enables LACP on the interface in a passive negotiating state. The port responds to LACP packets but cannot start LACP negotiations.</li>
</ul></li>
</ul>
Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 469.
<i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 403; Arista User Manual, v. 4.11.1 (1/11/13), at 336; Arista User Manual v. 4.10.3 (10/22/12), at 294; Arista User Manual v. 4.9.3.2 (5/3/12), at 278; Arista User Manual v. 4.8.2 (11/18/11), at 210; Arista User Manual v. 4.7.3 (7/18/11), at 424; Arista User Manual v. 4.6.0 (12/22/2010), at 271
</td>
</tr>
<tr>
<td>Cisco NX-OS 6.2
Effective date of registration: 11/13/2014</td>
<td>

<i>Table 6-1 Channel Modes for Individual Links in a Port Channel</i>
<table>
<tr><th>Channel Mode</th><th>Description</th></tr>
<tr><td>passive</td><td>LACP mode that places a port into a passive negotiating state in which the port responds to LACP packets that it receives but does not initiate LACP negotiation.</td></tr>
<tr><td>active</td><td>LACP mode that places a port into an active negotiating state in which the port initiates negotiations with other ports by sending LACP packets.</td></tr>
<tr><td>on</td><td>All static port channels (that are not running LACP) remain in this mode. If you attempt to change the channel mode to active or passive before enabling LACP, the device displays an error message.
You enable LACP on each channel by configuring the interface in that channel for the channel mode as either <b>active</b> or <b>passive</b>. When an LACP attempts to negotiate with an interface in the <b>on</b> state, it does not receive any LACP packets and becomes an individual link with that interface; it does not join the LACP channel group.
The default port-channel mode is <b>on</b>.</td></tr>
</table>
Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide, Release 6.x (2013), at 6-10
</td>
<td>

<ul>
<li><i>LACP_MODE</i> specifies the interface LACP mode. Values include:
<ul>
<li>— mode on Configures interface as a static port channel, disabling LACP. The switch does not verify or negotiate port channel membership with other switches.</li>
<li>— mode active Enables LACP on the interface in active negotiating state. The port initiates negotiations with other ports by sending LACP packets.</li>
<li>— mode passive Enables LACP on the interface in a passive negotiating state. The port responds to LACP packets but cannot start LACP negotiations.</li>
</ul></li>
</ul>
Arista User Manual v. 4.14.3F (Rev. 2) (October 2, 2014), at 469.
<i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 403; Arista User Manual, v. 4.11.1 (1/11/13), at 336; Arista User Manual v. 4.10.3 (10/22/12), at 294; Arista User Manual v. 4.9.3.2 (5/3/12), at 278; Arista User Manual v. 4.8.2 (11/18/11), at 210; Arista User Manual v. 4.7.3 (7/18/11), at 424; Arista User Manual v. 4.6.0 (12/22/2010), at 271
</td>
</tr>
</table>

<table>
<tr><th>Copyright Registration Information</th><th>Cisco</th><th>Arista</th></tr>
<tr>
<td>Cisco NX-OS 5.0
Effective date of registration: 11/13/2014</td>
<td>
Table 5-1 Channel Modes for Individual Links in a Port Channel
<table><tr><th>Channel Mode</th><th>Description</th></tr><tr><td>passive</td><td>LACP mode that places a port into a passive negotiating state in which the port responds to LACP packets that it receives but does not initiate LACP negotiation.</td></tr><tr><td>active</td><td>LACP mode that places a port into an active negotiating state in which the port initiates negotiations with other ports by sending LACP packets.</td></tr><tr><td>on</td><td>All static port channels (that are not running LACP) remain in this mode. If you attempt to change the channel mode to active or passive before enabling LACP, the device displays an error message.
You enable LACP on each channel by configuring the interface in that channel for the channel mode as either <b>active</b> or <b>passive</b>. When an LACP attempts to negotiate with an interface in the <b>on</b> state, it does not receive any LACP packets and becomes an individual link with that interface; it does not join the LACP channel group.
The default port-channel mode is <b>on</b>.</td></tr></table>
Interfaces Configuration Guide, Cisco DCNM for LAN, Release 5.x (2010), at 6-9</td>
<td>
Parameters
• <i>number</i> specifies a channel group ID. Values range from 1 through 1000.
• <i>LACP_MODE</i> specifies the interface LACP mode. Values include:
— mode on Configures interface as a static port channel, disabling LACP. The switch does not verify or negotiate port channel membership with other switches.
— mode active Enables LACP on the interface in active negotiating state. The port initiates negotiations with other ports by sending LACP packets.
— mode passive Enables LACP on the interface in a passive negotiating state. The port responds to LACP packets but cannot start LACP negotiations.
Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 469.
<i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 403; Arista User Manual, v. 4.11.1 (1/11/13), at 336; Arista User Manual v. 4.10.3 (10/22/12), at 294; Arista User Manual v. 4.9.3.2 (5/3/12), at 278; Arista User Manual v. 4.8.2 (11/18/11), at 210; Arista User Manual v. 4.7.3 (7/18/11), at 424; Arista User Manual v. 4.6.0 (12/22/2010), at 271</td>
</tr>
<tr>
<td>Cisco NX-OS 5.0
Effective date of registration: 11/13/2014</td>
<td>
Table 5-1 Channel Modes for Individual Links in a Port Channel
<table><tr><th>Channel Mode</th><th>Description</th></tr><tr><td>passive</td><td>LACP mode that places a port into a passive negotiating state in which the port responds to LACP packets that it receives but does not initiate LACP negotiation.</td></tr><tr><td>active</td><td>LACP mode that places a port into an active negotiating state in which the port initiates negotiations with other ports by sending LACP packets.</td></tr><tr><td>on</td><td>All static port channels (that are not running LACP) remain in this mode. If you attempt to change the channel mode to active or passive before enabling LACP, the device displays an error message.
You enable LACP on each channel by configuring the interface in that channel for the channel mode as either <b>active</b> or <b>passive</b>. When an LACP attempts to negotiate with an interface in the <b>on</b> state, it does not receive any LACP packets and becomes an individual link with that interface; it does not join the LACP channel group.
The default port-channel mode is <b>on</b>.</td></tr></table>
Interfaces Configuration Guide, Cisco DCNM for LAN, Release 4.x (2008), at 5-9</td>
<td>
Parameters
• <i>number</i> specifies a channel group ID. Values range from 1 through 1000.
• <i>LACP_MODE</i> specifies the interface LACP mode. Values include:
— mode on Configures interface as a static port channel, disabling LACP. The switch does not verify or negotiate port channel membership with other switches.
— mode active Enables LACP on the interface in active negotiating state. The port initiates negotiations with other ports by sending LACP packets.
— mode passive Enables LACP on the interface in a passive negotiating state. The port responds to LACP packets but cannot start LACP negotiations.
Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 469.
<i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 403; Arista User Manual, v. 4.11.1 (1/11/13), at 336; Arista User Manual v. 4.10.3 (10/22/12), at 294; Arista User Manual v. 4.9.3.2 (5/3/12), at 278; Arista User Manual v. 4.8.2 (11/18/11), at 210; Arista User Manual v. 4.7.3 (7/18/11), at 424; Arista User Manual v. 4.6.0 (12/22/2010), at 271</td>
</tr>
</table>

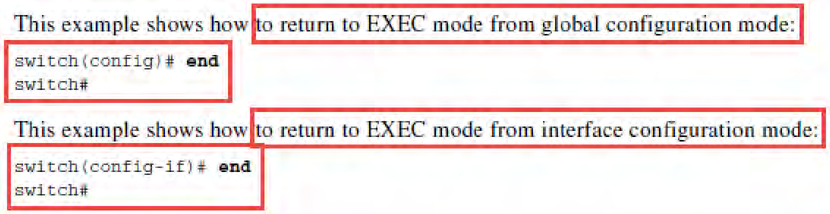
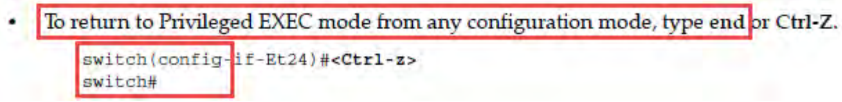
Copyright Registration Information	Cisco	Arista
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	 Note For information about configuring port channels and the Link Aggregation Control Protocol (LACP), see Chapter 5, "Configuring Port Channels." Interfaces Configuration Guide, Cisco DCNM for LAN, Release 6.x (2012), at 6-2	 **Port Channels and LACP** This chapter describes channel groups, port channels, port channel interfaces, and the Link Aggregation Control Protocol (LACP). This chapter contains the following sections: Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 469. *See also* Arista User Manual v. 4.12.3 (7/17/13), at 391; Arista User Manual, v. 4.11.1 (1/11/13), at 329; Arista User Manual v. 4.10.3 (10/22/12), at 287; Arista User Manual v. 4.9.3.2 (5/3/12), at 271; Arista User Manual v. 4.8.2 (11/18/11), at 203.
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	 Note For information about configuring port channels and the Link Aggregation Control Protocol (LACP), see Chapter 5, "Configuring Port Channels." Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide, Release 6.x (2013), at 7-1	 **Port Channels and LACP** This chapter describes channel groups, port channels, port channel interfaces, and the Link Aggregation Control Protocol (LACP). This chapter contains the following sections: Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 469. *See also* Arista User Manual v. 4.12.3 (7/17/13), at 391; Arista User Manual, v. 4.11.1 (1/11/13), at 329; Arista User Manual v. 4.10.3 (10/22/12), at 287; Arista User Manual v. 4.9.3.2 (5/3/12), at 271; Arista User Manual v. 4.8.2 (11/18/11), at 203.

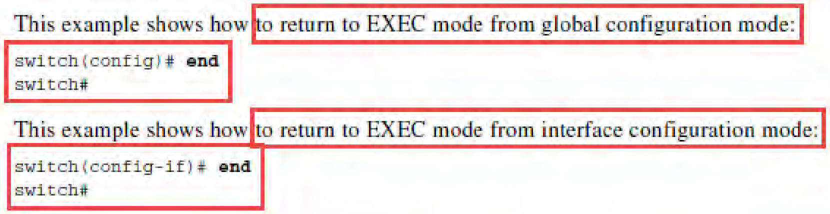
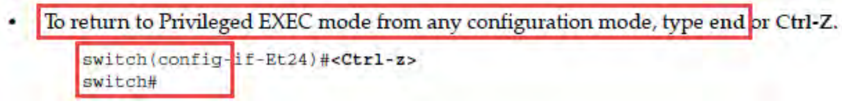
Copyright Registration Information	Cisco	Arista
Cisco NX-OS 5.0 Effective date of registration: 11/13/2014	 **Note** For information about configuring port channels and the Link Aggregation Control Protocol (LACP), see Chapter 5, "Configuring Port Channels." Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide, Release 5.x (2010), at 7-1	 **Port Channels and LACP** This chapter describes channel groups, port channels, port channel interfaces, and the Link Aggregation Control Protocol (LACP). This chapter contains the following sections: Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 469. *See also* Arista User Manual v. 4.12.3 (7/17/13), at 391; Arista User Manual, v. 4.11.1 (1/11/13), at 329; Arista User Manual v. 4.10.3 (10/22/12), at 287; Arista User Manual v. 4.9.3.2 (5/3/12), at 271; Arista User Manual v. 4.8.2 (11/18/11), at 203.
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	 **Loopback Interfaces** A loopback interface is a virtual interface with a single endpoint that is always up. Any packet transmitted over a loopback interface is immediately received by this interface. Loopback interfaces emulate a physical interface. You can configure up to 1024 loopback interfaces per VDC, numbered 0 to 1023. Interfaces Configuration Guide, Cisco DCNM for LAN, Release 6.x (2012), at 4-4 .	 **14.4.4 Loopback Ports** A loopback interface is a virtual network interface implemented in software and does not connect to any hardware. Traffic sent to the loopback interface is immediately received on the sending interface. The switch provides loopback configuration mode for creating loopback interfaces and modifying their operating parameters. Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 631. *See also* Arista User Manual v. 4.12.3 (7/17/13), at 500; Arista User Manual, v. 4.11.1 (1/11/13), at 397; Arista User Manual v. 4.10.3 (10/22/12), at 329.
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	 **Loopback Interfaces** A loopback interface is a virtual interface with a single endpoint that is always up. Any packet transmitted over a loopback interface is immediately received by this interface. Loopback interfaces emulate a physical interface. You can configure up to 1024 loopback interfaces per VDC, numbered 0 to 1023. Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide, Release 6.x (2013), at 4-4	 **14.4.4 Loopback Ports** A loopback interface is a virtual network interface implemented in software and does not connect to any hardware. Traffic sent to the loopback interface is immediately received on the sending interface. The switch provides loopback configuration mode for creating loopback interfaces and modifying their operating parameters. Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 631. *See also* Arista User Manual v. 4.12.3 (7/17/13), at 500; Arista User Manual, v. 4.11.1 (1/11/13), at 397; Arista User Manual v. 4.10.3 (10/22/12), at 329.

Copyright Registration Information	Cisco	Arista
Cisco NX-OS 5.0 Effective date of registration: 11/13/2014	 **Loopback Interfaces** A loopback interface is a virtual interface with a single endpoint that is always up. Any packet transmitted over a loopback interface is immediately received by this interface. Loopback interfaces emulate a physical interface. You can configure up to 1024 loopback interfaces per VDC, numbered 0 to 1023. Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide, Release 5.x (2010), at 4-4	 14.4.4 Loopback Ports A loopback interface is a virtual network interface implemented in software and does not connect to any hardware. Traffic sent to the loopback interface is immediately received on the sending interface. The switch provides loopback configuration mode for creating loopback interfaces and modifying their operating parameters. Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 631. *See also* Arista User Manual v. 4.12.3 (7/17/13), at 500; Arista User Manual, v. 4.11.1 (1/11/13), at 397; Arista User Manual v. 4.10.3 (10/22/12), at 329.
Cisco NX-OS 4.0 Effective date of registration: 11/13/2014	 **Loopback Interfaces** A loopback interface is a virtual interface with a single endpoint that is always up. Any packet transmitted over a loopback interface is immediately received by this interface. Loopback interfaces emulate a physical interface. You can configure up to 1024 loopback interfaces per VDC, numbered 0 to 1023. Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide, Release 4.x (2010), at 4-3	 14.4.4 Loopback Ports A loopback interface is a virtual network interface implemented in software and does not connect to any hardware. Traffic sent to the loopback interface is immediately received on the sending interface. The switch provides loopback configuration mode for creating loopback interfaces and modifying their operating parameters. Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 631. *See also* Arista User Manual v. 4.12.3 (7/17/13), at 500; Arista User Manual, v. 4.11.1 (1/11/13), at 397; Arista User Manual v. 4.10.3 (10/22/12), at 329.
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	 **Configuring a Maximum Number of MAC Addresses** You can configure the maximum number of MAC addresses that can be learned or statically configured on interfaces that belong to a port profile. Interfaces Configuration Guide, Cisco DCNM for LAN, Release 6.x (2012), at 10-22	 **Port Security Configuration** MAC security restricts input to a switched port by limiting the number and identity of MAC addresses that can access the port. MAC address security is enabled by switchport port-security. Ports with MAC security enabled restrict traffic to a limited number of hosts, as determined by their MAC addresses. The maximum number of MAC addresses that can be assigned to an interface is configured by switchport port-security maximum. The default MAC address limit on an interface where port security is enabled is one. Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 632. *See also* Arista User Manual v. 4.13.6F (4/14/2014), at 624; Arista User Manual v. 4.12.3 (7/17/13), at 501; Arista User Manual, v. 4.11.1 (1/11/13), at 405; Arista User Manual v. 4.10.3 (10/22/12), at 336.

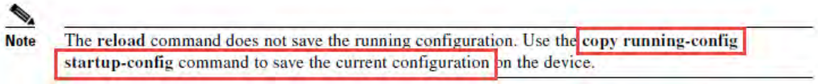
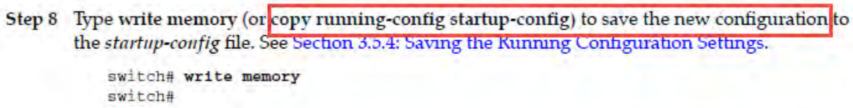
Copyright Registration Information	Cisco	Arista
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	 By default, an interface can have only one secure MAC address. You can configure the maximum number of MAC addresses permitted per interface or per VLAN on an interface. Maximums apply to secure MAC addresses learned by any method: dynamic, sticky, or static. ICisco Nexus 7000 Series NX-OS Security Configuration Guide, Release 6.x (2013), at 507	 **Port Security Configuration** MAC security restricts input to a switched port by limiting the number and identity of MAC addresses that can access the port. MAC address security is enabled by switchport port-security. Ports with MAC security enabled restrict traffic to a limited number of hosts, as determined by their MAC addresses. The maximum number of MAC addresses that can be assigned to an interface is configured by switchport port-security maximum. The default MAC address limit on an interface where port security is enabled is one. Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 632. *See also* Arista User Manual v. 4.13.6F (4/14/2014), at 624; Arista User Manual v. 4.12.3 (7/17/13), at 501; Arista User Manual, v. 4.11.1 (1/11/13), at 405; Arista User Manual v. 4.10.3 (10/22/12), at 336.
Cisco NX-OS 5.0 Effective date of registration: 11/13/2014	 By default, an interface can have only one secure MAC address. You can configure the maximum number of MAC addresses permitted per interface or per VLAN on an interface. Maximums apply to secure MAC addresses learned by any method: dynamic, sticky, or static. Cisco Nexus 7000 Series NX-OS Security Configuration Guide, Release 5.x (2010), at 177	 **Port Security Configuration** MAC security restricts input to a switched port by limiting the number and identity of MAC addresses that can access the port. MAC address security is enabled by switchport port-security. Ports with MAC security enabled restrict traffic to a limited number of hosts, as determined by their MAC addresses. The maximum number of MAC addresses that can be assigned to an interface is configured by switchport port-security maximum. The default MAC address limit on an interface where port security is enabled is one. Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 632. *See also* Arista User Manual v. 4.13.6F (4/14/2014), at 624; Arista User Manual v. 4.12.3 (7/17/13), at 501; Arista User Manual, v. 4.11.1 (1/11/13), at 405; Arista User Manual v. 4.10.3 (10/22/12), at 336.

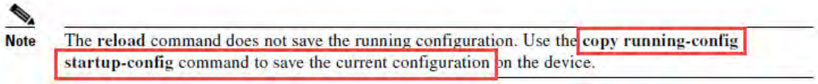
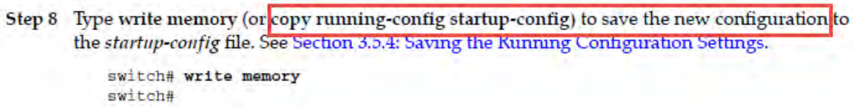
Copyright Registration Information	Cisco	Arista

Cisco NX-OS 6.2
Effective date of registration: 11/13/2014
	
	This example shows how to return to EXEC mode from global configuration mode:
	`switch(config)# end`
	`switch#`
	This example shows how to return to EXEC mode from interface configuration mode:
	`switch(config-if)# end`
	`switch#`
	Cisco Nexus 7000 Series NX-OS Fundamentals Command Reference (2013), at FND-44
		
		• To return to Privileged EXEC mode from any configuration mode, type end or Ctrl-Z.
		`switch(config-if-Et24)#<Ctrl-z>`
		`switch#`
		Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 120.
		See also Arista User Manual v. 4.12.3 (7/17/13), at 99; Arista User Manual, v. 4.11.1 (1/11/13), at 69; Arista User Manual v. 4.10.3 (10/22/12), at 61; Arista User Manual v. 4.9.3.2 (5/3/12), at 57; Arista User Manual v. 4.8.2 (11/18/11), at 52; Arista User Manual v. 4.7.3 (7/18/11), at 47; Arista User Manual v. 4.6.0 (12/22/2010), at 41

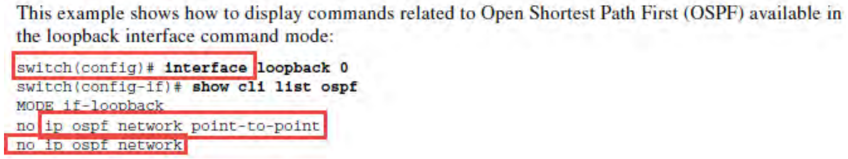
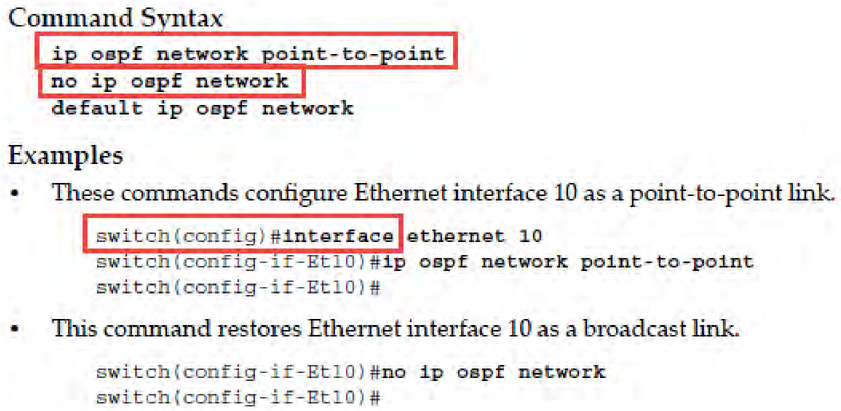
Cisco NX-OS 5.0
Effective date of registration: 11/13/2014
	
	This example shows how to return to EXEC mode from global configuration mode:
	`switch(config)# end`
	`switch#`
	This example shows how to return to EXEC mode from interface configuration mode:
	`switch(config-if)# end`
	`switch#`
	Cisco Nexus 7000 Series NX-OS Fundamentals Command Reference (2010), at FND-37
		
		• To return to Privileged EXEC mode from any configuration mode, type end or Ctrl-Z.
		`switch(config-if-Et24)#<Ctrl-z>`
		`switch#`
		Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 120.
		See also Arista User Manual v. 4.12.3 (7/17/13), at 99; Arista User Manual, v. 4.11.1 (1/11/13), at 69; Arista User Manual v. 4.10.3 (10/22/12), at 61; Arista User Manual v. 4.9.3.2 (5/3/12), at 57; Arista User Manual v. 4.8.2 (11/18/11), at 52; Arista User Manual v. 4.7.3 (7/18/11), at 47; Arista User Manual v. 4.6.0 (12/22/2010), at 41

Copyright Registration Information	Cisco	Arista

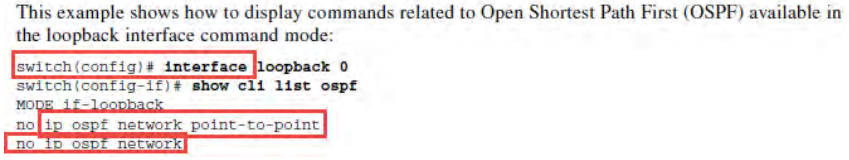
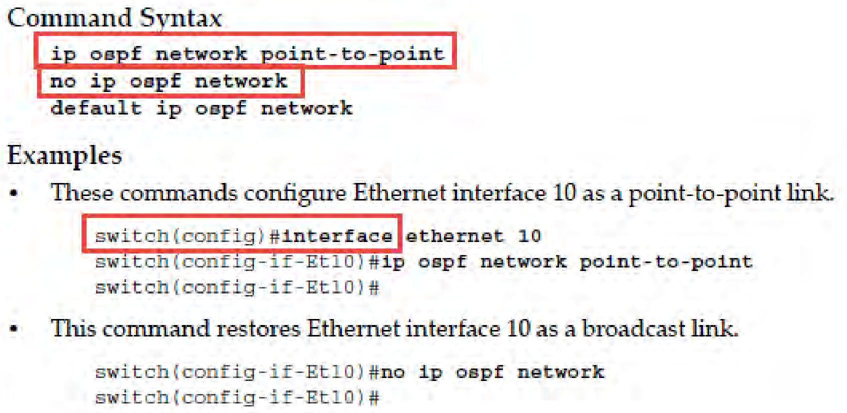
Cisco NX-OS 6.2
Effective date of registration: 11/13/2014
	
	Note The **reload** command does not save the running configuration. Use the **copy running-config startup-config** command to save the current configuration on the device.
	Cisco Nexus 7000 Series NX-OS Fundamentals Command Reference (2013), at FND-105
		
		Step 8 Type **write memory** (or **copy running-config startup-config**) to save the new configuration to the *startup-config* file. See Section 3.5.4: Saving the Running Configuration Settings.
		`switch# write memory`
		`switch#`
		Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 60.
		See also Arista User Manual v. 4.12.3 (7/17/13), at 52; Arista User Manual, v. 4.11.1 (1/11/13), at 44; Arista User Manual v. 4.10.3 (10/22/12), at 38; Arista User Manual v. 4.9.3.2 (5/3/12), at 34; Arista User Manual v. 4.8.2 (11/18/11), at 30; Arista User Manual v. 4.7.3 (7/18/11), at 28; Arista User Manual v. 4.6.0 (12/22/2010), at 25

Cisco NX-OS 5.0
Effective date of registration: 11/13/2014
	
	Note The **reload** command does not save the running configuration. Use the **copy running-config startup-config** command to save the current configuration on the device.
	Cisco Nexus 7000 Series NX-OS Fundamentals Command Reference (2010), at FND-84
		
		Step 8 Type **write memory** (or **copy running-config startup-config**) to save the new configuration to the *startup-config* file. See Section 3.5.4: Saving the Running Configuration Settings.
		`switch# write memory`
		`switch#`
		Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 60.
		See also Arista User Manual v. 4.12.3 (7/17/13), at 52; Arista User Manual, v. 4.11.1 (1/11/13), at 44; Arista User Manual v. 4.10.3 (10/22/12), at 38; Arista User Manual v. 4.9.3.2 (5/3/12), at 34; Arista User Manual v. 4.8.2 (11/18/11), at 30; Arista User Manual v. 4.7.3 (7/18/11), at 28; Arista User Manual v. 4.6.0 (12/22/2010), at 25

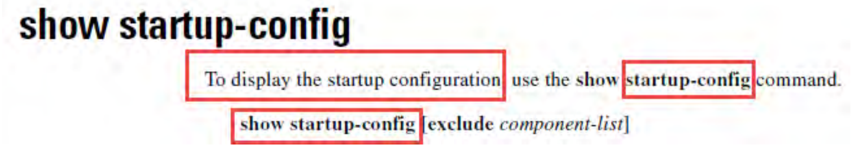
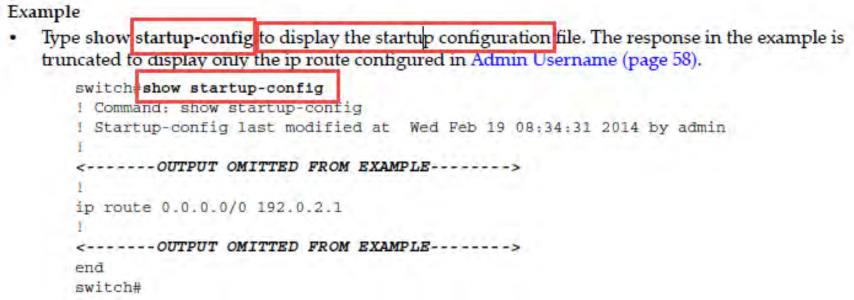
Copyright Registration Information	Cisco	Arista

Cisco NX-OS 6.2
Effective date of registration: 11/13/2014
	
	This example shows how to display commands related to Open Shortest Path First (OSPF) available in the loopback interface command mode:
	`switch(config)# interface loopback 0`
	`switch(config-if)# show cli list ospf`
	`MODE if-loopback`
	`no ip ospf network point-to-point`
	`no ip ospf network`
	Cisco Nexus 7000 Series NX-OS Fundamentals Command Reference (2013), at FND-126
		
		Command Syntax
		`ip ospf network point-to-point`
		`no ip ospf network`
		`default ip ospf network`
		Examples
		• These commands configure Ethernet interface 10 as a point-to-point link.
		`switch(config)#interface ethernet 10`
		`switch(config-if-Et10)#ip ospf network point-to-point`
		`switch(config-if-Et10)#`
		• This command restores Ethernet interface 10 as a broadcast link.
		`switch(config-if-Et10)#no ip ospf network`
		`switch(config-if-Et10)#`
		Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 1432.
		See also Arista User Manual v. 4.12.3 (7/17/13), at 1219; Arista User Manual, v. 4.11.1 (1/11/13), at 976; Arista User Manual v. 4.10.3 (10/22/12), at 806; Arista User Manual v. 4.9.3.2 (5/3/12), at 692; Arista User Manual v. 4.8.2 (11/18/11), at 465; Arista User Manual v. 4.7.3 (7/18/11), at 338.

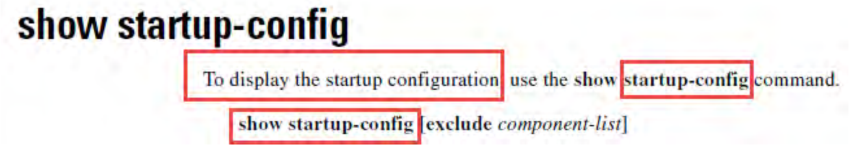
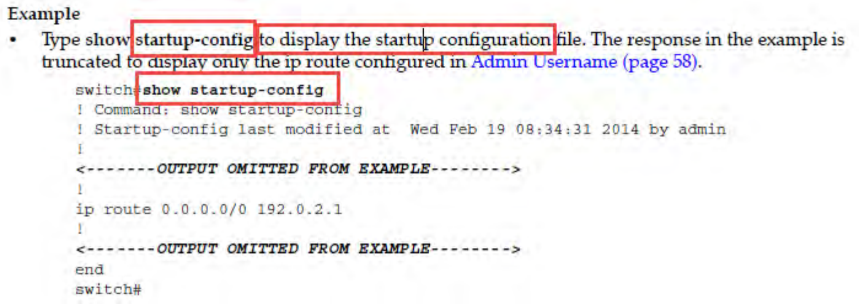
Copyright Registration Information	Cisco	Arista

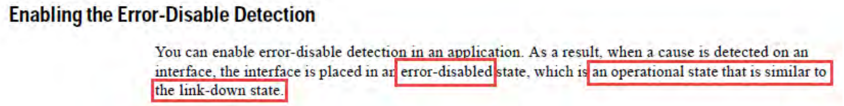
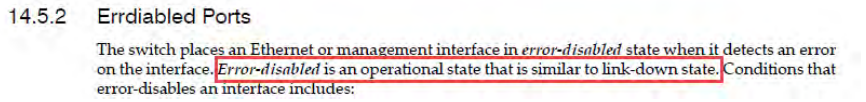
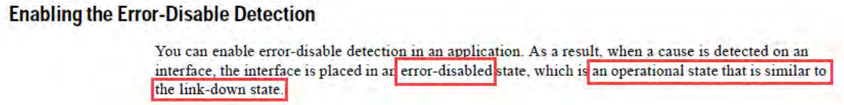
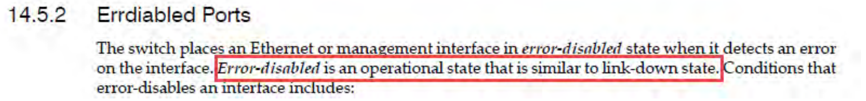
Cisco NX-OS 5.0
Effective date of registration: 11/13/2014
	
	This example shows how to display commands related to Open Shortest Path First (OSPF) available in the loopback interface command mode:
	`switch(config)# interface loopback 0`
	`switch(config-if)# show cli list ospf`
	`MODE if-loopback`
	`no ip ospf network point-to-point`
	`no ip ospf network`
	Cisco Nexus 7000 Series NX-OS Fundamentals Command Reference (2010), at FND-105
		
		Command Syntax
		`ip ospf network point-to-point`
		`no ip ospf network`
		`default ip ospf network`
		Examples
		• These commands configure Ethernet interface 10 as a point-to-point link.
		`switch(config)#interface ethernet 10`
		`switch(config-if-Et10)#ip ospf network point-to-point`
		`switch(config-if-Et10)#`
		• This command restores Ethernet interface 10 as a broadcast link.
		`switch(config-if-Et10)#no ip ospf network`
		`switch(config-if-Et10)#`
		Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 1432.
		See also Arista User Manual v. 4.12.3 (7/17/13), at 1219; Arista User Manual, v. 4.11.1 (1/11/13), at 976; Arista User Manual v. 4.10.3 (10/22/12), at 806; Arista User Manual v. 4.9.3.2 (5/3/12), at 692; Arista User Manual v. 4.8.2 (11/18/11), at 465; Arista User Manual v. 4.7.3 (7/18/11), at 338.

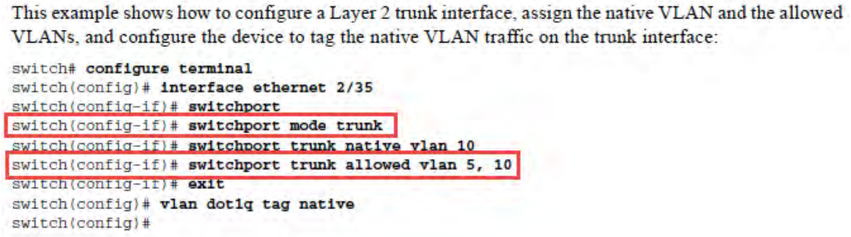
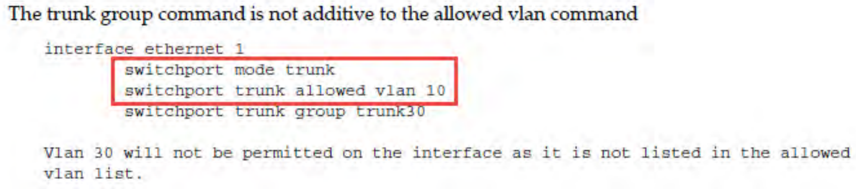
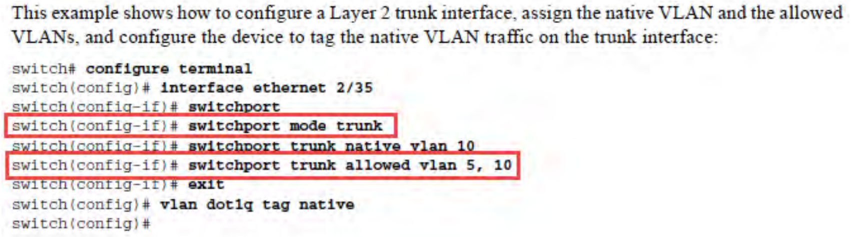
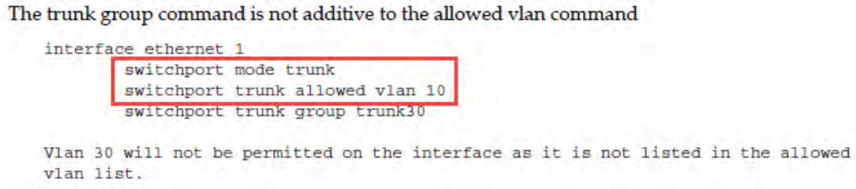
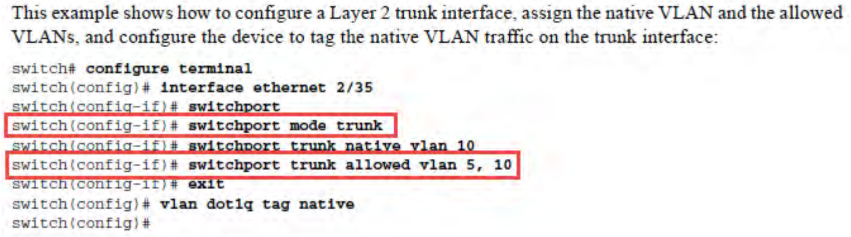
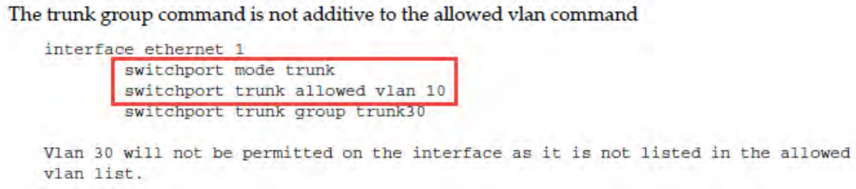
Copyright Registration Information	Cisco	Arista

Cisco NX-OS 6.2
Effective date of registration: 11/13/2014
	
	show startup-config
	To display the startup configuration use the show startup-config command.
	show startup-config [**exclude** *component-list*]
	Cisco Nexus 7000 Series NX-OS Fundamentals Command Reference (2013), at FND-154.
		
		Example
		• Type show startup-config to display the startup configuration file. The response in the example is truncated to display only the ip route configured in Admin Username (page 58).
		`switch#show startup-config`
		`! Command: show startup-config`
		`! Startup-config last modified at  Wed Feb 19 08:34:31 2014 by admin`
		`!`
		`<-------OUTPUT OMITTED FROM EXAMPLE-------->`
		`!`
		`ip route 0.0.0.0/0 192.0.2.1`
		`!`
		`<-------OUTPUT OMITTED FROM EXAMPLE-------->`
		`end`
		`switch#`
		Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 123.
		See also Arista User Manual v. 4.12.3 (7/17/13), at 102; Arista User Manual, v. 4.11.1 (1/11/13), at 72; Arista User Manual v. 4.10.3 (10/22/12), at 65; Arista User Manual v. 4.9.3.2 (5/3/12), at 59; Arista User Manual v. 4.8.2 (11/18/11), at 54; Arista User Manual v. 4.7.3 (7/18/11), at 49.

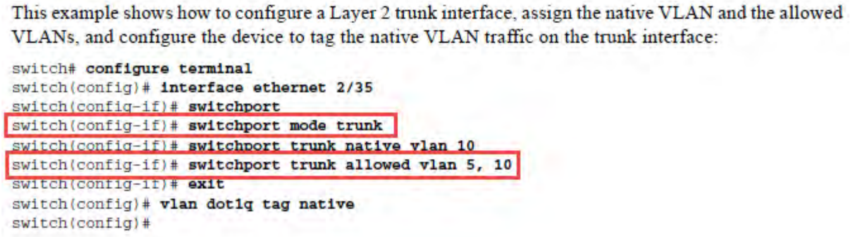
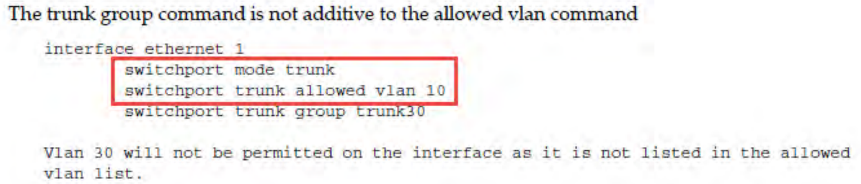
Copyright Registration Information	Cisco	Arista

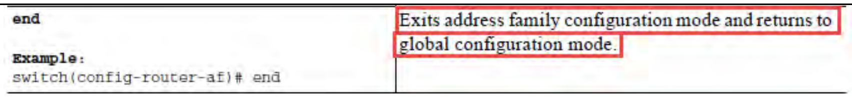
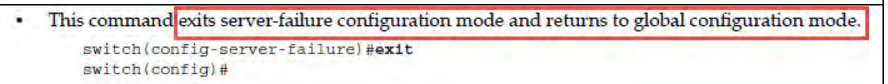
Cisco NX-OS 6.2
Effective date of registration: 11/13/2014
	
	show startup-config
	To display the startup configuration, use the **show startup-config** command.
	show startup-config [**exclude** *component-list*]
	Cisco Nexus 7000 Series NX-OS Fundamentals Command Reference (2010), at FND-125.
		
		Example
		• Type show startup-config to display the startup configuration file. The response in the example is truncated to display only the ip route configured in Admin Username (page 58).
		`switch#show startup-config`
		`! Command: show startup-config`
		`! Startup-config last modified at  Wed Feb 19 08:34:31 2014 by admin`
		`!`
		`<-------OUTPUT OMITTED FROM EXAMPLE-------->`
		`!`
		`ip route 0.0.0.0/0 192.0.2.1`
		`!`
		`<-------OUTPUT OMITTED FROM EXAMPLE-------->`
		`end`
		`switch#`
		Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 123.
		See also Arista User Manual v. 4.12.3 (7/17/13), at 102; Arista User Manual, v. 4.11.1 (1/11/13), at 72; Arista User Manual v. 4.10.3 (10/22/12), at 65; Arista User Manual v. 4.9.3.2 (5/3/12), at 59; Arista User Manual v. 4.8.2 (11/18/11), at 54; Arista User Manual v. 4.7.3 (7/18/11), at 49.

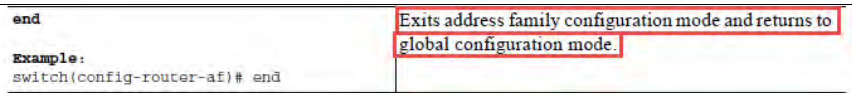
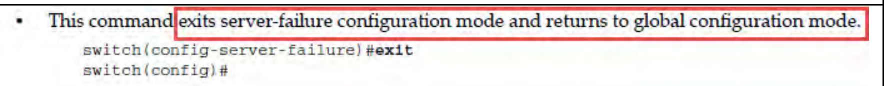
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	 **Enabling the Error-Disable Detection** You can enable error-disable detection in an application. As a result, when a cause is detected on an interface, the interface is placed in an error-disabled state, which is an operational state that is similar to the link-down state. Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide, Release 6.x (2013), at 2-24.	 14.5.2 Errdiabled Ports The switch places an Ethernet or management interface in *error-disabled* state when it detects an error on the interface. *Error-disabled* is an operational state that is similar to link-down state. Conditions that error-disables an interface includes: Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 123. *See also* Arista User Manual v. 4.12.3 (7/17/13), at 503.
Cisco NX-OS 5.2 Effective date of registration: 11/13/2014	 **Enabling the Error-Disable Detection** You can enable error-disable detection in an application. As a result, when a cause is detected on an interface, the interface is placed in an error-disabled state, which is an operational state that is similar to the link-down state. Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide, Release 5.x (2011), at 2-22.	 14.5.2 Errdiabled Ports The switch places an Ethernet or management interface in *error-disabled* state when it detects an error on the interface. *Error-disabled* is an operational state that is similar to link-down state. Conditions that error-disables an interface includes: Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 123. *See also* Arista User Manual v. 4.12.3 (7/17/13), at 503.

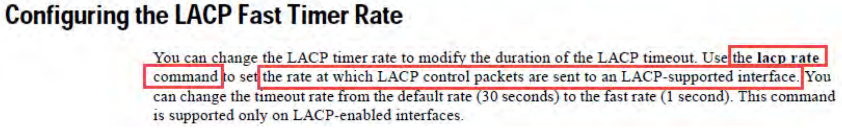
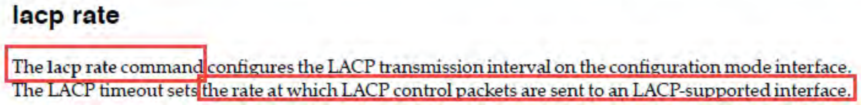
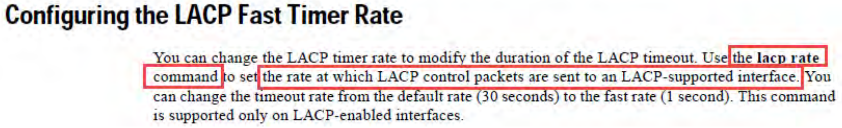
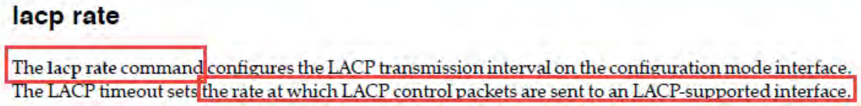
Copyright Registration Information	Cisco	Arista
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	 This example shows how to configure a Layer 2 trunk interface, assign the native VLAN and the allowed VLANs, and configure the device to tag the native VLAN traffic on the trunk interface: switch# **configure terminal** switch(config)# **interface ethernet 2/35** switch(config-if)# **switchport** switch(config-if)# **switchport mode trunk** switch(config-if)# **switchport trunk native vlan 10** switch(config-if)# **switchport trunk allowed vlan 5, 10** switch(config-if)# **exit** switch(config)# **vlan dot1q tag native** switch(config)# Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide, Release 6.x (2013), at 3-36.	 The trunk group command is not additive to the allowed vlan command interface ethernet 1 switchport mode trunk switchport trunk allowed vlan 10 switchport trunk group trunk30 Vlan 30 will not be permitted on the interface as it is not listed in the allowed vlan list. Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 767.
Cisco NX-OS 5.2 Effective date of registration: 11/13/2014	 This example shows how to configure a Layer 2 trunk interface, assign the native VLAN and the allowed VLANs, and configure the device to tag the native VLAN traffic on the trunk interface: switch# **configure terminal** switch(config)# **interface ethernet 2/35** switch(config-if)# **switchport** switch(config-if)# **switchport mode trunk** switch(config-if)# **switchport trunk native vlan 10** switch(config-if)# **switchport trunk allowed vlan 5, 10** switch(config-if)# **exit** switch(config)# **vlan dot1q tag native** switch(config)# Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide, Release 5.x (2011), at 3-23-24.	 The trunk group command is not additive to the allowed vlan command interface ethernet 1 switchport mode trunk switchport trunk allowed vlan 10 switchport trunk group trunk30 Vlan 30 will not be permitted on the interface as it is not listed in the allowed vlan list. Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 767.
Cisco NX-OS 5.0 Effective date of registration: 11/13/2014	 This example shows how to configure a Layer 2 trunk interface, assign the native VLAN and the allowed VLANs, and configure the device to tag the native VLAN traffic on the trunk interface: switch# **configure terminal** switch(config)# **interface ethernet 2/35** switch(config-if)# **switchport** switch(config-if)# **switchport mode trunk** switch(config-if)# **switchport trunk native vlan 10** switch(config-if)# **switchport trunk allowed vlan 5, 10** switch(config-if)# **exit** switch(config)# **vlan dot1q tag native** switch(config)# Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide, Release 5.x (2010), at 3-19.	 The trunk group command is not additive to the allowed vlan command interface ethernet 1 switchport mode trunk switchport trunk allowed vlan 10 switchport trunk group trunk30 Vlan 30 will not be permitted on the interface as it is not listed in the allowed vlan list. Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 767.

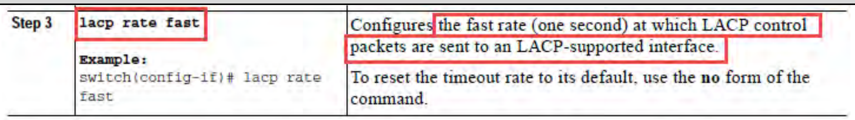
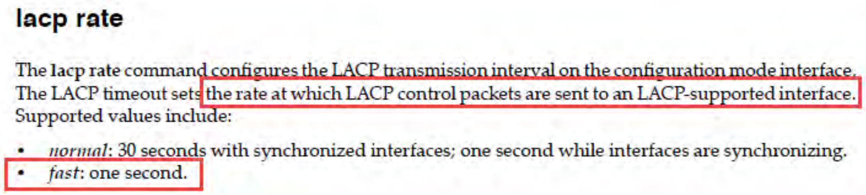
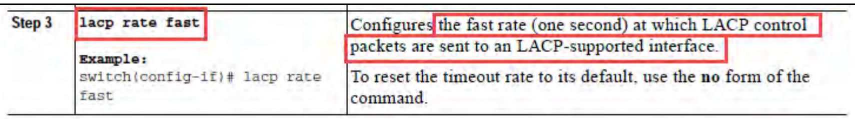
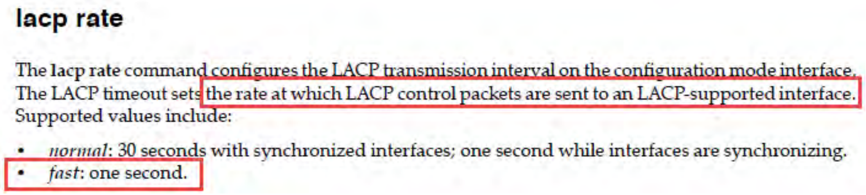
Copyright Registration Information	Cisco	Arista

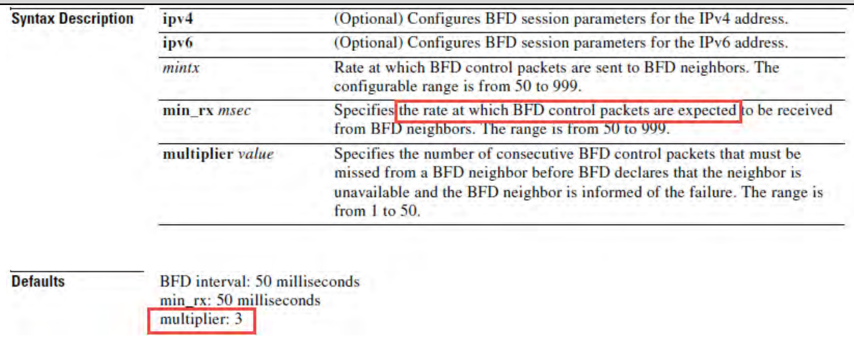
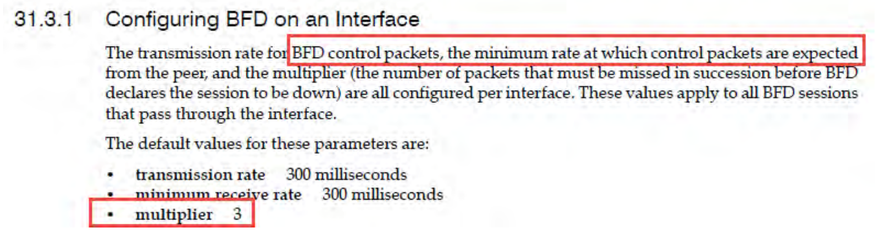
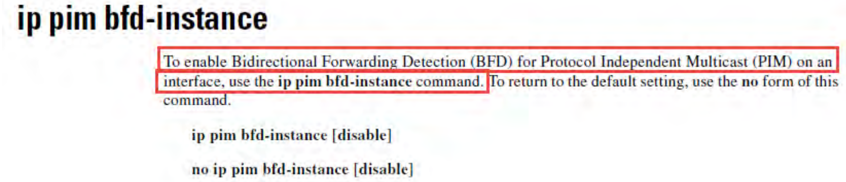
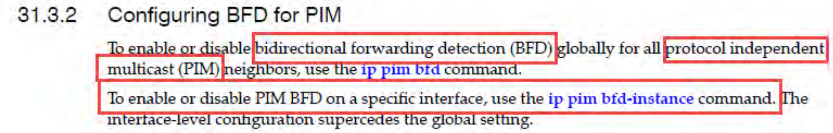
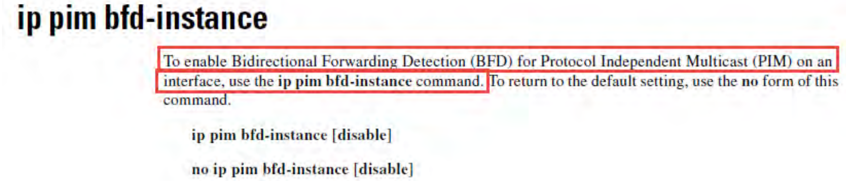
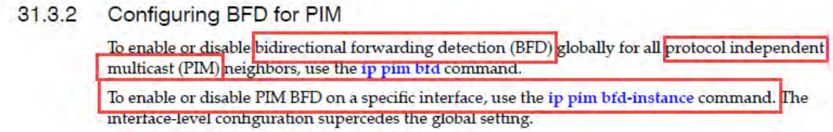
Cisco NX-OS 4.0
Effective date of registration: 11/13/2014
	
	This example shows how to configure a Layer 2 trunk interface, assign the native VLAN and the allowed VLANs, and configure the device to tag the native VLAN traffic on the trunk interface:
	`switch# configure terminal`
	`switch(config)# interface ethernet 2/35`
	`switch(config-if)# switchport`
	`switch(config-if)# switchport mode trunk`
	`switch(config-if)# switchport trunk native vlan 10`
	`switch(config-if)# switchport trunk allowed vlan 5, 10`
	`switch(config-if)# exit`
	`switch(config)# vlan dot1q tag native`
	`switch(config)#`
	Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide, Release 5.x (2008), at 3-17.
		
		The trunk group command is not additive to the allowed vlan command
		`interface ethernet 1`
		`    switchport mode trunk`
		`    switchport trunk allowed vlan 10`
		`    switchport trunk group trunk30`
		`Vlan 30 will not be permitted on the interface as it is not listed in the allowed vlan list.`
		Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 767.

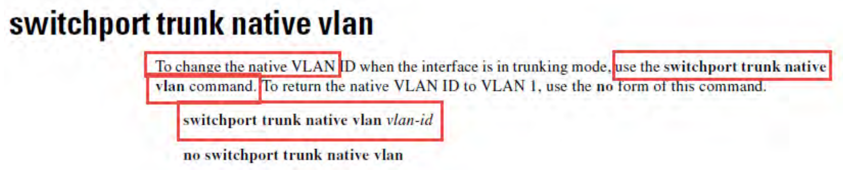
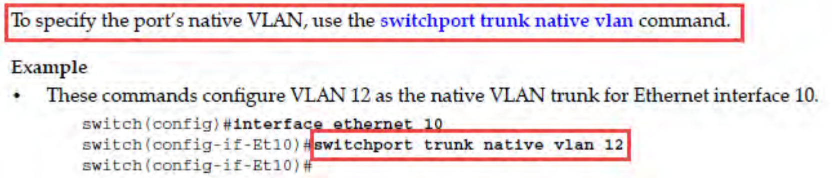
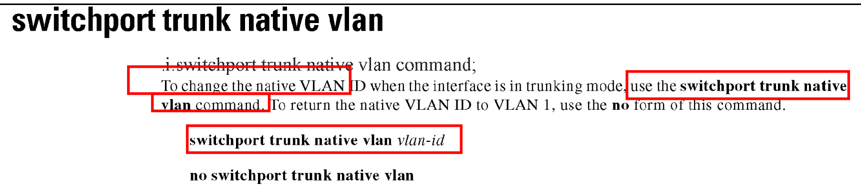
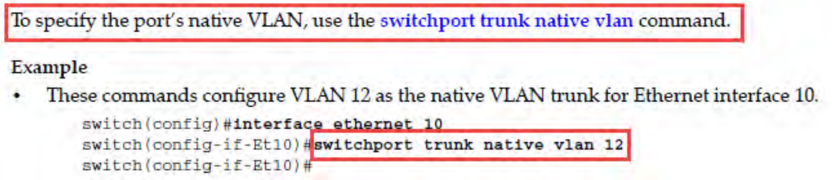
Cisco NX-OS 6.2
Effective date of registration: 11/13/2014
	
	end | Exits address family configuration mode and returns to global configuration mode.
	Example:
	`switch(config-router-af)# end`
	Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide, Release 6.x (2013), at 5-30.
		
		• This command exits server-failure configuration mode and returns to global configuration mode.
		`switch(config-server-failure)#exit`
		`switch(config)#`
		Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 640.
		See also Arista User Manual v. 4.12.3 (7/17/13), at 508.

Cisco IOS 15.0
Effective date of registration: 11/28/2014
	
	end | Exits address family configuration mode and returns to global configuration mode.
	Example:
	`switch(config-router-af)# end`
	Cisco IOS IP Multicast Configuration Guide (2009), at 289.
		
		• This command exits server-failure configuration mode and returns to global configuration mode.
		`switch(config-server-failure)#exit`
		`switch(config)#`
		Arista User Manual v. 4.14.3F - Rev. 2 (10/2/14), at 640.
		See also Arista User Manual v. 4.12.3 (7/17/13), at 508.

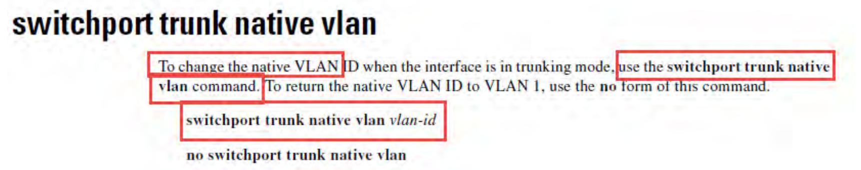
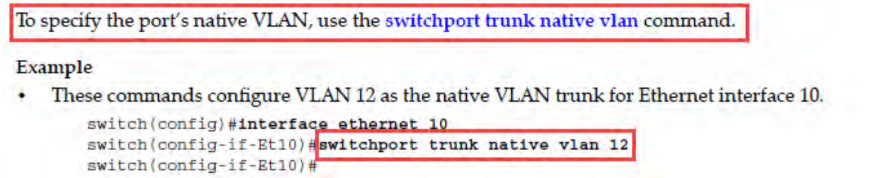
Copyright Registration Information	Cisco	Arista
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	 **Configuring the LACP Fast Timer Rate** You can change the LACP timer rate to modify the duration of the LACP timeout. Use the **lacp rate command** to set the rate at which LACP control packets are sent to an LACP-supported interface. You can change the timeout rate from the default rate (30 seconds) to the fast rate (1 second). This command is supported only on LACP-enabled interfaces. Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide, Release 6.x (2013), at 6-38,	 **lacp rate** The lacp rate command configures the LACP transmission interval on the configuration mode interface. The LACP timeout sets the rate at which LACP control packets are sent to an LACP-supported interface. Arista User Manual v. 4.14.3F (Rev. 2) (October 2, 2014), at 478. *See also* Arista User Manual v. 4.12.3 (7/17/13), at 395; Arista User Manual, v. 4.11.1 (1/11/13), at 340; Arista User Manual v. 4.10.3 (10/22/12), at 298; Arista User Manual v. 4.9.3.2 (5/3/12), at 275; Arista User Manual v. 4.8.2 (11/18/11), at 213.
Cisco NX-OS 5.2 Effective date of registration: 11/13/2014	 **Configuring the LACP Fast Timer Rate** You can change the LACP timer rate to modify the duration of the LACP timeout. Use the **lacp rate command** to set the rate at which LACP control packets are sent to an LACP-supported interface. You can change the timeout rate from the default rate (30 seconds) to the fast rate (1 second). This command is supported only on LACP-enabled interfaces. Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide, Release 5.x (June 14, 2011), at 6-333.	 **lacp rate** The lacp rate command configures the LACP transmission interval on the configuration mode interface. The LACP timeout sets the rate at which LACP control packets are sent to an LACP-supported interface. Arista User Manual v. 4.14.3F (Rev. 2) (October 2, 2014), at 478. *See also* Arista User Manual v. 4.12.3 (7/17/13), at 395; Arista User Manual, v. 4.11.1 (1/11/13), at 340; Arista User Manual v. 4.10.3 (10/22/12), at 298; Arista User Manual v. 4.9.3.2 (5/3/12), at 275; Arista User Manual v. 4.8.2 (11/18/11), at 213.

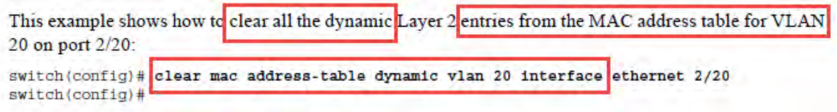
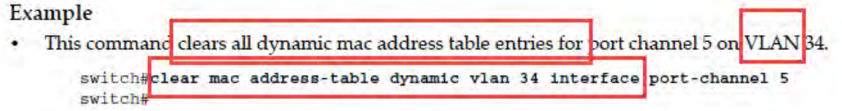
Copyright Registration Information	Cisco	Arista
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	 Step 3 — **lacp rate fast** **Example:** `switch(config-if)# lacp rate fast` Configures the fast rate (one second) at which LACP control packets are sent to an LACP-supported interface. To reset the timeout rate to its default, use the **no** form of the command. Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide, Release 6.x (2013), at 6-38.	 **lacp rate** The lacp rate command configures the LACP transmission interval on the configuration mode interface. The LACP timeout sets the rate at which LACP control packets are sent to an LACP-supported interface. Supported values include: • *normal*: 30 seconds with synchronized interfaces; one second while interfaces are synchronizing. • *fast*: one second. Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 478. *See also* Arista User Manual v. 4.12.3 (7/17/13), at 395; Arista User Manual, v. 4.11.1 (1/11/13), at 340; Arista User Manual v. 4.10.3 (10/22/12), at 298; Arista User Manual v. 4.9.3.2 (5/3/12), at 275; Arista User Manual v. 4.8.2 (11/18/11), at 213.
Cisco NX-OS 5.2 Effective date of registration: 11/13/2014	 Step 3 — **lacp rate fast** **Example:** `switch(config-if)# lacp rate fast` Configures the fast rate (one second) at which LACP control packets are sent to an LACP-supported interface. To reset the timeout rate to its default, use the **no** form of the command. Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide, Release 5.x (June 14, 2011), at 6-34.	 **lacp rate** The lacp rate command configures the LACP transmission interval on the configuration mode interface. The LACP timeout sets the rate at which LACP control packets are sent to an LACP-supported interface. Supported values include: • *normal*: 30 seconds with synchronized interfaces; one second while interfaces are synchronizing. • *fast*: one second. Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 478. *See also* Arista User Manual v. 4.12.3 (7/17/13), at 395; Arista User Manual, v. 4.11.1 (1/11/13), at 340; Arista User Manual v. 4.10.3 (10/22/12), at 298; Arista User Manual v. 4.9.3.2 (5/3/12), at 275; Arista User Manual v. 4.8.2 (11/18/11), at 213.

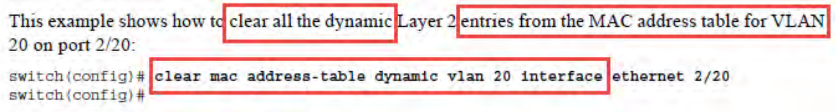
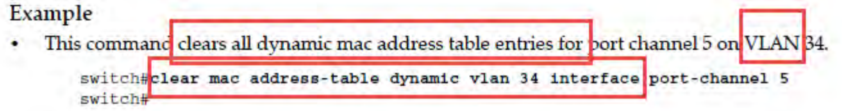
Copyright Registration Information	Cisco	Arista
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	 **Syntax Description** **ipv4** (Optional) Configures BFD session parameters for the IPv4 address. **ipv6** (Optional) Configures BFD session parameters for the IPv6 address. *mintx* Rate at which BFD control packets are sent to BFD neighbors. The configurable range is from 50 to 999. **min_rx** *msec* Specifies the rate at which BFD control packets are expected to be received from BFD neighbors. The range is from 50 to 999. **multiplier** *value* Specifies the number of consecutive BFD control packets that must be missed from a BFD neighbor before BFD declares that the neighbor is unavailable and the BFD neighbor is informed of the failure. The range is from 1 to 50. **Defaults** BFD interval: 50 milliseconds min_rx: 50 milliseconds multiplier: 3 Cisco Nexus 7000 Series NX-OS Interfaces Command Reference, Release 6.x (2013), at 1-12.	 31.3.1 Configuring BFD on an Interface The transmission rate for BFD control packets, the minimum rate at which control packets are expected from the peer, and the multiplier (the number of packets that must be missed in succession before BFD declares the session to be down) are all configured per interface. These values apply to all BFD sessions that pass through the interface. The default values for these parameters are: • **transmission rate** 300 milliseconds • **minimum receive rate** 300 milliseconds • **multiplier** 3 Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 1737. *See also* Arista User Manual v. 4.12.3 (7/17/13), at 1467.
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	 **ip pim bfd-instance** To enable Bidirectional Forwarding Detection (BFD) for Protocol Independent Multicast (PIM) on an interface, use the **ip pim bfd-instance** command. To return to the default setting, use the **no** form of this command. **ip pim bfd-instance [disable]** **no ip pim bfd-instance [disable]** Cisco Nexus 7000 Series NX-OS Interfaces Command Reference, Release 6.x (2013), at 1-251.	 31.3.2 Configuring BFD for PIM To enable or disable bidirectional forwarding detection (BFD) globally for all protocol independent multicast (PIM) neighbors, use the ip pim bfd command. To enable or disable PIM BFD on a specific interface, use the ip pim bfd-instance command. The interface-level configuration supercedes the global setting. Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 766. *See also* Arista User Manual v. 4.12.3 (7/17/13), at 1467.
Cisco NX-OS 5.0 Effective date of registration: 11/13/2014	 **ip pim bfd-instance** To enable Bidirectional Forwarding Detection (BFD) for Protocol Independent Multicast (PIM) on an interface, use the **ip pim bfd-instance** command. To return to the default setting, use the **no** form of this command. **ip pim bfd-instance [disable]** **no ip pim bfd-instance [disable]** Cisco Nexus 7000 Series NX-OS Interfaces Command Reference, Release 5.x (2010), at 66.	 31.3.2 Configuring BFD for PIM To enable or disable bidirectional forwarding detection (BFD) globally for all protocol independent multicast (PIM) neighbors, use the ip pim bfd command. To enable or disable PIM BFD on a specific interface, use the ip pim bfd-instance command. The interface-level configuration supercedes the global setting. Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 766. *See also* Arista User Manual v. 4.12.3 (7/17/13), at 1467.

Copyright Registration Information	Cisco	Arista
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	 **switchport trunk native vlan** To change the native VLAN ID when the interface is in trunking mode, use the **switchport trunk native vlan** command. To return the native VLAN ID to VLAN 1, use the **no** form of this command. **switchport trunk native vlan** *vlan-id* **no switchport trunk native vlan** Cisco Nexus 7000 Series NX-OS Interfaces Command Reference, Release 6.x (2013), at 1-253.	 To specify the port's native VLAN, use the switchport trunk native vlan command. **Example** • These commands configure VLAN 12 as the native VLAN trunk for Ethernet interface 10. `switch(config)#`**`interface ethernet 10`** `switch(config-if-Et10)#`**`switchport trunk native vlan 12`** `switch(config-if-Et10)#` Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 766. *See also* Arista User Manual v. 4.12.3 (7/17/13), at 614; Arista User Manual, v. 4.11.1 (1/11/13), at 470; Arista User Manual v. 4.10.3 (10/22/12), at 390; Arista User Manual v. 4.9.3.2 (5/3/12), at 310.
Cisco NX-OS 5.0 Effective date of registration: 11/13/2014	 **switchport trunk native vlan** .i.switchport trunk native vlan command; To change the native VLAN ID when the interface is in trunking mode, use the **switchport trunk native vlan** command. To return the native VLAN ID to VLAN 1, use the **no** form of this command. **switchport trunk native vlan** *vlan-id* **no switchport trunk native vlan** Cisco Nexus 7000 Series NX-OS Interfaces Command Reference, Release 5.x (2010), at 222.	 To specify the port's native VLAN, use the switchport trunk native vlan command. **Example** • These commands configure VLAN 12 as the native VLAN trunk for Ethernet interface 10. `switch(config)#`**`interface ethernet 10`** `switch(config-if-Et10)#`**`switchport trunk native vlan 12`** `switch(config-if-Et10)#` Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 766. *See also* Arista User Manual v. 4.12.3 (7/17/13), at 614; Arista User Manual, v. 4.11.1 (1/11/13), at 470; Arista User Manual v. 4.10.3 (10/22/12), at 390; Arista User Manual v. 4.9.3.2 (5/3/12), at 310.

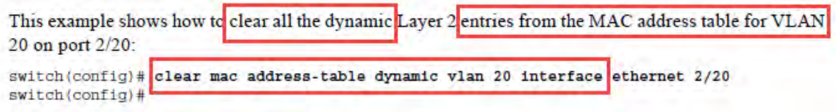
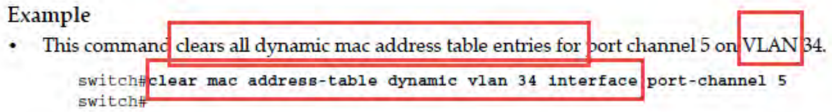
Copyright Registration Information	Cisco	Arista

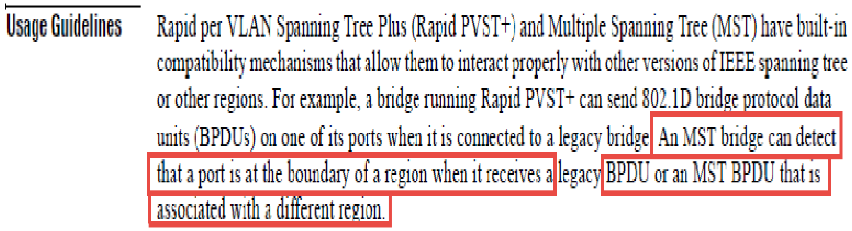
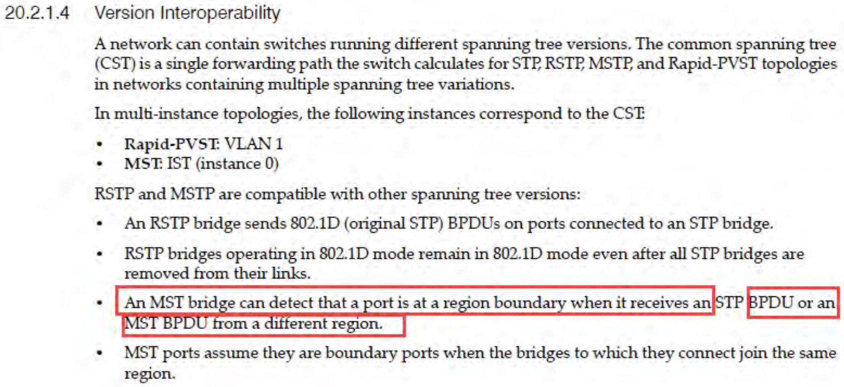
Cisco NX-OS 4.0
Effective date of registration: 11/13/2014
	
	switchport trunk native vlan
	To change the native VLAN ID when the interface is in trunking mode, use the **switchport trunk native vlan** command. To return the native VLAN ID to VLAN 1, use the **no** form of this command.
	switchport trunk native vlan *vlan-id*
	no switchport trunk native vlan
	Cisco Nexus 7000 Series NX-OS Interfaces Command Reference, Release 4.0 (2008), at IF-35.
		
		To specify the port's native VLAN, use the switchport trunk native vlan command.
		Example
		• These commands configure VLAN 12 as the native VLAN trunk for Ethernet interface 10.
		`switch(config)#interface ethernet 10`
		`switch(config-if-Et10)#switchport trunk native vlan 12`
		`switch(config-if-Et10)#`
		Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 766.
		See also Arista User Manual v. 4.12.3 (7/17/13), at 614; Arista User Manual, v. 4.11.1 (1/11/13), at 470; Arista User Manual v. 4.10.3 (10/22/12), at 390; Arista User Manual v. 4.9.3.2 (5/3/12), at 310.

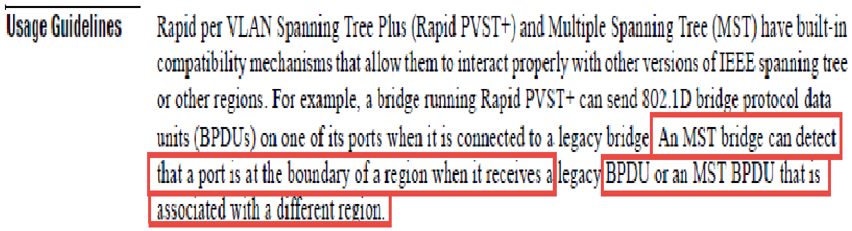
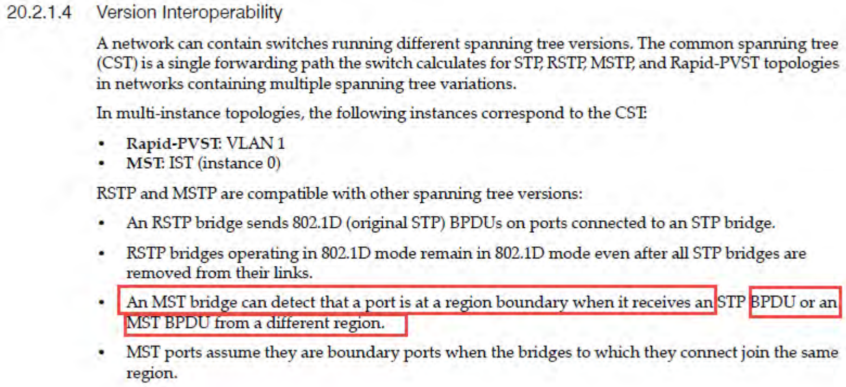
Cisco NX-OS 6.2
Effective date of registration: 11/13/2014
	
	This example shows how to clear all the dynamic Layer 2 entries from the MAC address table for VLAN 20 on port 2/20:
	`switch(config)# clear mac address-table dynamic vlan 20 interface ethernet 2/20`
	`switch(config)#`
	Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference, (2013), at 3.
		
		Example
		• This command clears all dynamic mac address table entries for port channel 5 on VLAN 34.
		`switch#clear mac address-table dynamic vlan 34 interface port-channel 5`
		`switch#`
		Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 648.
		See also Arista User Manual v. 4.12.3 (7/17/13), at 516; Arista User Manual, v. 4.11.1 (1/11/13), at 402; Arista User Manual v. 4.10.3 (10/22/12), at 333; Arista User Manual v. 4.9.3.2 (5/3/12), at 316.

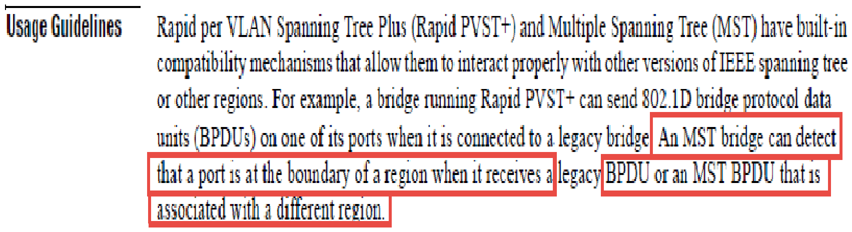
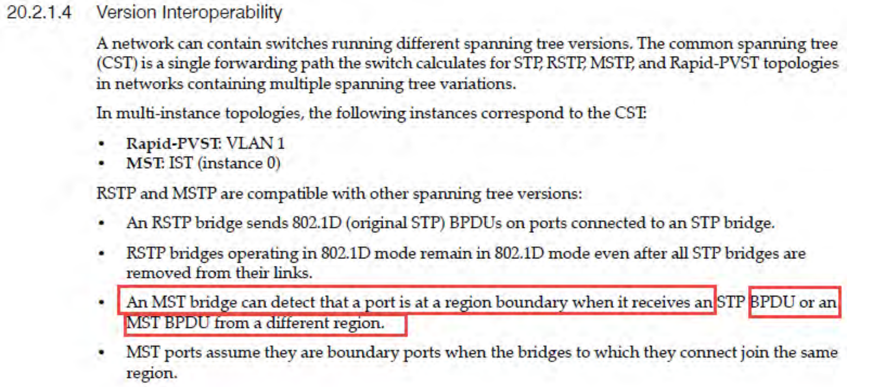
Cisco NX-OS 5.0
Effective date of registration: 11/13/2014
	
	This example shows how to clear all the dynamic Layer 2 entries from the MAC address table for VLAN 20 on port 2/20:
	`switch(config)# clear mac address-table dynamic vlan 20 interface ethernet 2/20`
	`switch(config)#`
	Cisco NX-OS Layer 2 Switching Command Reference, Release 5.x (2010), at L2-2-L2-3.
		
		Example
		• This command clears all dynamic mac address table entries for port channel 5 on VLAN 34.
		`switch#clear mac address-table dynamic vlan 34 interface port-channel 5`
		`switch#`
		Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 648.
		See also Arista User Manual v. 4.12.3 (7/17/13), at 516; Arista User Manual, v. 4.11.1 (1/11/13), at 402; Arista User Manual v. 4.10.3 (10/22/12), at 333; Arista User Manual v. 4.9.3.2 (5/3/12), at 316.

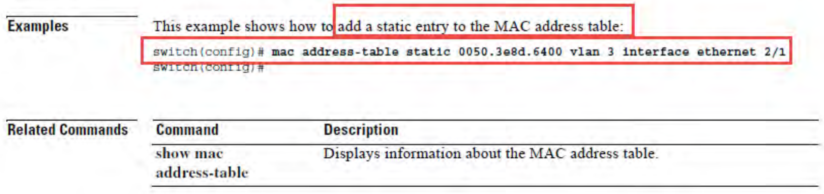
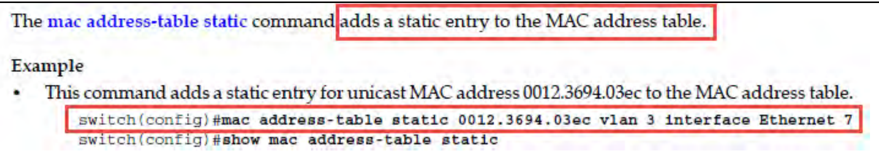
Copyright Registration Information	Cisco	Arista

Cisco NX-OS 4.0
Effective date of registration: 11/13/2014
	
	This example shows how to clear all the dynamic Layer 2 entries from the MAC address table for VLAN 20 on port 2/20:
	`switch(config)# clear mac address-table dynamic vlan 20 interface ethernet 2/20`
	`switch(config)#`
	Cisco NX-OS Layer 2 Switching Command Reference, Release 4.0 (2008), at L2-2-L2-3.
		
		Example
		• This command clears all dynamic mac address table entries for port channel 5 on VLAN 34.
		`switch#clear mac address-table dynamic vlan 34 interface port-channel 5`
		`switch#`
		Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 648.
		See also Arista User Manual v. 4.12.3 (7/17/13), at 516; Arista User Manual, v. 4.11.1 (1/11/13), at 402; Arista User Manual v. 4.10.3 (10/22/12), at 333; Arista User Manual v. 4.9.3.2 (5/3/12), at 316.

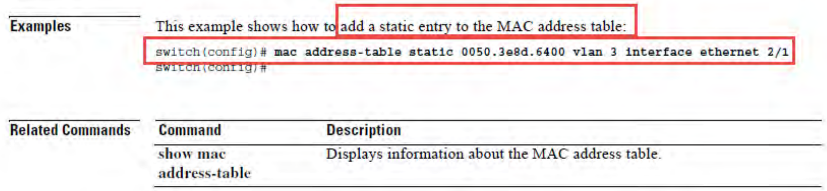
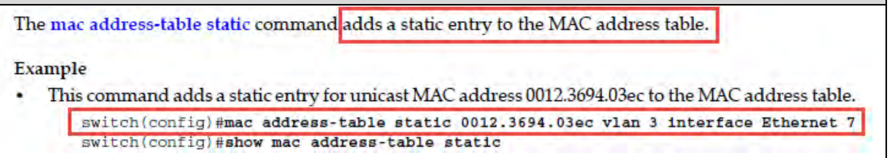
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	 Usage Guidelines Rapid per VLAN Spanning Tree Plus (Rapid PVST+) and Multiple Spanning Tree (MST) have built-in compatibility mechanisms that allow them to interact properly with other versions of IEEE spanning tree or other regions. For example, a bridge running Rapid PVST+ can send 802.1D bridge protocol data units (BPDUs) on one of its ports when it is connected to a legacy bridge. An MST bridge can detect that a port is at the boundary of a region when it receives a legacy BPDU or an MST BPDU that is associated with a different region. Cisco Nexus 7000 Series NX-OS Interfaces Command Reference, Release 6.x (2013), at 5.	 20.2.1.4 Version Interoperability A network can contain switches running different spanning tree versions. The common spanning tree (CST) is a single forwarding path the switch calculates for STP, RSTP, MSTP, and Rapid-PVST topologies in networks containing multiple spanning tree variations. In multi-instance topologies, the following instances correspond to the CST: • Rapid-PVST: VLAN 1 • MST: IST (instance 0) RSTP and MSTP are compatible with other spanning tree versions: • An RSTP bridge sends 802.1D (original STP) BPDUs on ports connected to an STP bridge. • RSTP bridges operating in 802.1D mode remain in 802.1D mode even after all STP bridges are removed from their links. • An MST bridge can detect that a port is at a region boundary when it receives an STP BPDU or an MST BPDU from a different region. • MST ports assume they are boundary ports when the bridges to which they connect join the same region. Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 953. *See also* Arista User Manual v. 4.12.3 (7/17/13), at 831; Arista User Manual, v. 4.11.1 (1/11/13), at 649; Arista User Manual v. 4.10.3 (10/22/12), at 563; Arista User Manual v. 4.9.3.2 (5/3/12), at 483; Arista User Manual v. 4.8.2 (11/18/11), at 357; Arista User Manual v. 4.7.3 (7/18/11), at 231.

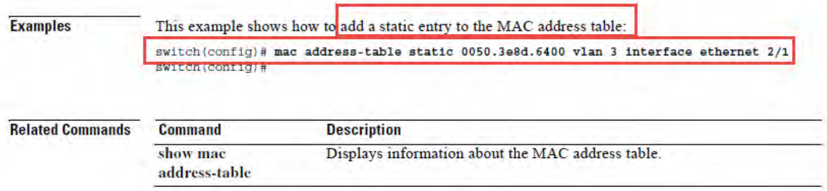
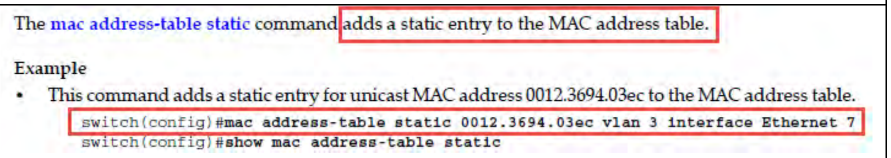
Copyright Registration Information	Cisco	Arista
Cisco NX-OS 5.0 Effective date of registration: 11/13/2014	 **Usage Guidelines** Rapid per VLAN Spanning Tree Plus (Rapid PVST+) and Multiple Spanning Tree (MST) have built-in compatibility mechanisms that allow them to interact properly with other versions of IEEE spanning tree or other regions. For example, a bridge running Rapid PVST+ can send 802.1D bridge protocol data units (BPDUs) on one of its ports when it is connected to a legacy bridge. An MST bridge can detect that a port is at the boundary of a region when it receives a legacy BPDU or an MST BPDU that is associated with a different region. Cisco NX-OS Layer 2 Switching Command Reference, Release 5.0 (2010), at L2-5.	 20.2.1.4 Version Interoperability A network can contain switches running different spanning tree versions. The common spanning tree (CST) is a single forwarding path the switch calculates for STP, RSTP, MSTP, and Rapid-PVST topologies in networks containing multiple spanning tree variations. In multi-instance topologies, the following instances correspond to the CST: • Rapid-PVST: VLAN 1 • MST: IST (instance 0) RSTP and MSTP are compatible with other spanning tree versions: • An RSTP bridge sends 802.1D (original STP) BPDUs on ports connected to an STP bridge. • RSTP bridges operating in 802.1D mode remain in 802.1D mode even after all STP bridges are removed from their links. • An MST bridge can detect that a port is at a region boundary when it receives an STP BPDU or an MST BPDU from a different region. • MST ports assume they are boundary ports when the bridges to which they connect join the same region. Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 953. *See also* Arista User Manual v. 4.12.3 (7/17/13), at 831; Arista User Manual, v. 4.11.1 (1/11/13), at 649; Arista User Manual v. 4.10.3 (10/22/12), at 563; Arista User Manual v. 4.9.3.2 (5/3/12), at 483; Arista User Manual v. 4.8.2 (11/18/11), at 357; Arista User Manual v. 4.7.3 (7/18/11), at 231.

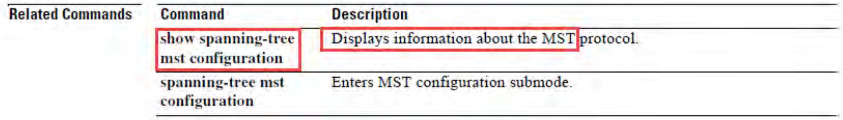
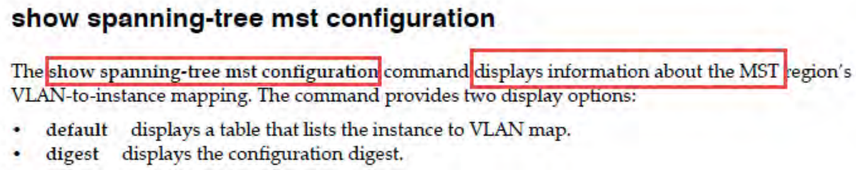
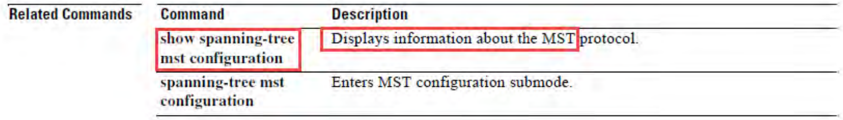
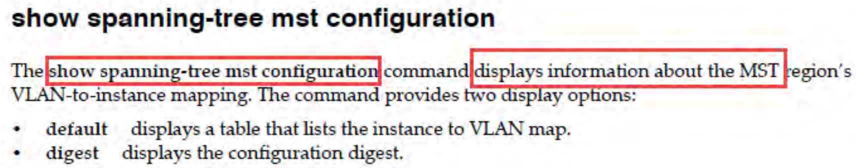
Copyright Registration Information	Cisco	Arista
Cisco NX-OS 4.0 Effective date of registration: 11/13/2014	 **Usage Guidelines** Rapid per VLAN Spanning Tree Plus (Rapid PVST+) and Multiple Spanning Tree (MST) have built-in compatibility mechanisms that allow them to interact properly with other versions of IEEE spanning tree or other regions. For example, a bridge running Rapid PVST+ can send 802.1D bridge protocol data units (BPDUs) on one of its ports when it is connected to a legacy bridge. An MST bridge can detect that a port is at the boundary of a region when it receives a legacy BPDU or an MST BPDU that is associated with a different region. Cisco NX-OS Layer 2 Switching Command Reference, Release 4.0 (2008), at L2-5.	 20.2.1.4 Version Interoperability A network can contain switches running different spanning tree versions. The common spanning tree (CST) is a single forwarding path the switch calculates for STP, RSTP, MSTP, and Rapid-PVST topologies in networks containing multiple spanning tree variations. In multi-instance topologies, the following instances correspond to the CST: • Rapid-PVST: VLAN 1 • MST: IST (instance 0) RSTP and MSTP are compatible with other spanning tree versions: • An RSTP bridge sends 802.1D (original STP) BPDUs on ports connected to an STP bridge. • RSTP bridges operating in 802.1D mode remain in 802.1D mode even after all STP bridges are removed from their links. • An MST bridge can detect that a port is at a region boundary when it receives an STP BPDU or an MST BPDU from a different region. • MST ports assume they are boundary ports when the bridges to which they connect join the same region. Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 953. *See also* Arista User Manual v. 4.12.3 (7/17/13), at 831; Arista User Manual, v. 4.11.1 (1/11/13), at 649; Arista User Manual v. 4.10.3 (10/22/12), at 563; Arista User Manual v. 4.9.3.2 (5/3/12), at 483; Arista User Manual v. 4.8.2 (11/18/11), at 357; Arista User Manual v. 4.7.3 (7/18/11), at 231.

Cisco NX-OS 6.2
Effective date of registration: 11/13/2014
	
	Examples
	This example shows how to add a static entry to the MAC address table:
	`switch(config)# mac address-table static 0050.3e8d.6400 vlan 3 interface ethernet 2/1`
	`switch(config)#`
	Related Commands
	Command: show mac address-table — Description: Displays information about the MAC address table.
	Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference (2013), at 20.
		
		The mac address-table static command adds a static entry to the MAC address table.
		Example
		• This command adds a static entry for unicast MAC address 0012.3694.03ec to the MAC address table.
		`switch(config)#mac address-table static 0012.3694.03ec vlan 3 interface Ethernet 7`
		`switch(config)#show mac address-table static`
		Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 624.
		See also Arista User Manual v. 4.12.3 (7/17/13), at 494; Arista User Manual, v. 4.11.1 (1/11/13), at 427-28; Arista User Manual, v. 4.11.1 (1/11/13), at; Arista User Manual v. 4.10.3 (10/22/12), at 331; Arista User Manual v. 4.9.3.2 (5/3/12), at 321-22.

Copyright Registration Information	Cisco	Arista

Cisco NX-OS 5.0
Effective date of registration: 11/13/2014
	
	Examples This example shows how to add a static entry to the MAC address table:
	`switch(config)# mac address-table static 0050.3e8d.6400 vlan 3 interface ethernet 2/1`
	`switch(config)#`
	Related Commands **Command** **Description**
	show mac address-table Displays information about the MAC address table.
	Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference, Release 5.x (2010), at L2-18.
		
		The mac address-table static command adds a static entry to the MAC address table.
		Example
		• This command adds a static entry for unicast MAC address 0012.3694.03ec to the MAC address table.
		`switch(config)#mac address-table static 0012.3694.03ec vlan 3 interface Ethernet 7`
		`switch(config)#show mac address-table static`
		Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 624.
		See also Arista User Manual v. 4.12.3 (7/17/13), at 494; Arista User Manual, v. 4.11.1 (1/11/13), at 427-28; Arista User Manual, v. 4.11.1 (1/11/13), at; Arista User Manual v. 4.10.3 (10/22/12), at 331; Arista User Manual v. 4.9.3.2 (5/3/12), at 321-22.

Cisco NX-OS 4.0
Effective date of registration: 11/13/2014
	
	Examples This example shows how to add a static entry to the MAC address table:
	`switch(config)# mac address-table static 0050.3e8d.6400 vlan 3 interface ethernet 2/1`
	`switch(config)#`
	Related Commands **Command** **Description**
	show mac address-table Displays information about the MAC address table.
	Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference, Release 4.0 (2008), at L2-13.
		
		The mac address-table static command adds a static entry to the MAC address table.
		Example
		• This command adds a static entry for unicast MAC address 0012.3694.03ec to the MAC address table.
		`switch(config)#mac address-table static 0012.3694.03ec vlan 3 interface Ethernet 7`
		`switch(config)#show mac address-table static`
		Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 624.
		See also Arista User Manual v. 4.12.3 (7/17/13), at 494; Arista User Manual, v. 4.11.1 (1/11/13), at 427-28; Arista User Manual, v. 4.11.1 (1/11/13), at; Arista User Manual v. 4.10.3 (10/22/12), at 331; Arista User Manual v. 4.9.3.2 (5/3/12), at 321-22.

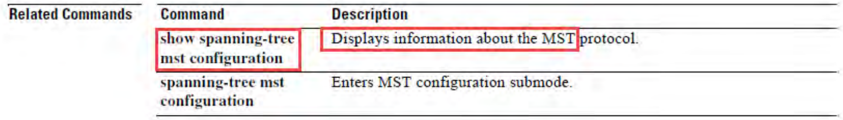
Copyright Registration Information	Cisco	Arista
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	 Related Commands Command / Description show spanning-tree mst configuration / Displays information about the MST protocol. spanning-tree mst configuration / Enters MST configuration submode. Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference (2013), at 24.	 **show spanning-tree mst configuration** The show spanning-tree mst configuration command displays information about the MST region's VLAN-to-instance mapping. The command provides two display options: • **default** displays a table that lists the instance to VLAN map. • **digest** displays the configuration digest. Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 991. *See also* Arista User Manual v. 4.12.3 (7/17/13), at 869; Arista User Manual, v. 4.11.1 (1/11/13), at 687; Arista User Manual v. 4.10.3 (10/22/12), at 601; Arista User Manual v. 4.9.3.2 (5/3/12), at 520; Arista User Manual v. 4.8.2 (11/18/11), at 394; Arista User Manual v. 4.7.3 (7/18/11), at 283.
Cisco NX-OS 5.0 Effective date of registration: 11/13/2014	 Related Commands Command / Description show spanning-tree mst configuration / Displays information about the MST protocol. spanning-tree mst configuration / Enters MST configuration submode. Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference, Release 5.x (2010), at L2-26.	 **show spanning-tree mst configuration** The show spanning-tree mst configuration command displays information about the MST region's VLAN-to-instance mapping. The command provides two display options: • **default** displays a table that lists the instance to VLAN map. • **digest** displays the configuration digest. Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 991. *See also* Arista User Manual v. 4.12.3 (7/17/13), at 869; Arista User Manual, v. 4.11.1 (1/11/13), at 687; Arista User Manual v. 4.10.3 (10/22/12), at 601; Arista User Manual v. 4.9.3.2 (5/3/12), at 520; Arista User Manual v. 4.8.2 (11/18/11), at 394; Arista User Manual v. 4.7.3 (7/18/11), at 283.

<table>
<tr><th>Copyright Registration Information</th><th>Cisco</th><th>Arista</th></tr>
<tr>
<td>

Cisco NX-OS 4.0

Effective date of registration: 11/13/2014

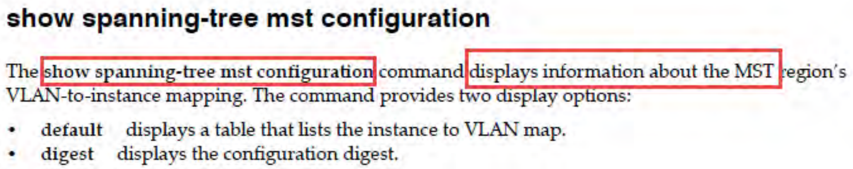
</td>
<td>



<table>
<tr><th>Related Commands</th><th>Command</th><th>Description</th></tr>
<tr><td></td><td>show spanning-tree mst configuration</td><td>Displays information about the MST protocol.</td></tr>
<tr><td></td><td>spanning-tree mst configuration</td><td>Enters MST configuration submode.</td></tr>
</table>

Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference, Release 4.x (2008), at L2-17.

</td>
<td>



show spanning-tree mst configuration

The show spanning-tree mst configuration command displays information about the MST region's VLAN-to-instance mapping. The command provides two display options:

- **default** displays a table that lists the instance to VLAN map.
- **digest** displays the configuration digest.

Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 991.

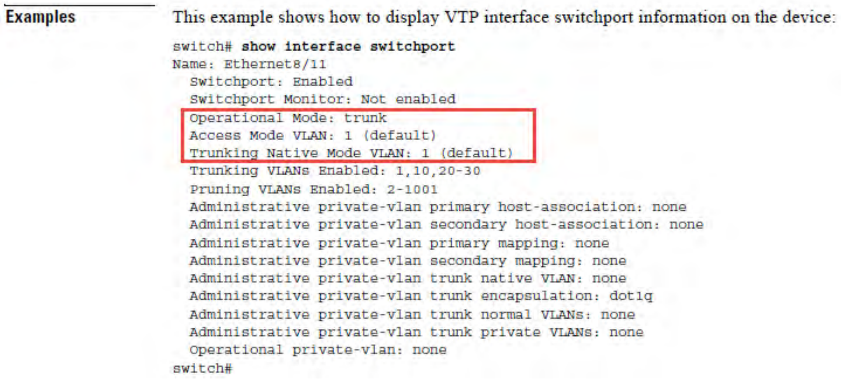
See also Arista User Manual v. 4.12.3 (7/17/13), at 869; Arista User Manual, v. 4.11.1 (1/11/13), at 687; Arista User Manual v. 4.10.3 (10/22/12), at 601; Arista User Manual v. 4.9.3.2 (5/3/12), at 520; Arista User Manual v. 4.8.2 (11/18/11), at 394; Arista User Manual v. 4.7.3 (7/18/11), at 283.

</td>
</tr>
<tr>
<td>

Cisco NX-OS 6.2

Effective date of registration: 11/13/2014

</td>
<td>

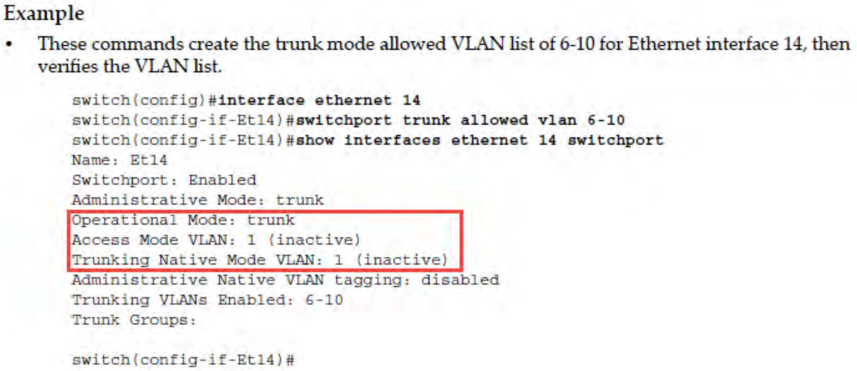


Examples This example shows how to display VTP interface switchport information on the device:

```
switch# show interface switchport
Name: Ethernet8/11
  Switchport: Enabled
  Switchport Monitor: Not enabled
  Operational Mode: trunk
  Access Mode VLAN: 1 (default)
  Trunking Native Mode VLAN: 1 (default)
  Trunking VLANs Enabled: 1,10,20-30
  Pruning VLANs Enabled: 2-1001
  Administrative private-vlan primary host-association: none
  Administrative private-vlan secondary host-association: none
  Administrative private-vlan primary mapping: none
  Administrative private-vlan secondary mapping: none
  Administrative private-vlan trunk native VLAN: none
  Administrative private-vlan trunk encapsulation: dot1q
  Administrative private-vlan trunk normal VLANs: none
  Administrative private-vlan trunk private VLANs: none
  Operational private-vlan: none
switch#
```

Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference (2013), at 44.

</td>
<td>



Example

- These commands create the trunk mode allowed VLAN list of 6-10 for Ethernet interface 14, then verifies the VLAN list.

```
switch(config)#interface ethernet 14
switch(config-if-Et14)#switchport trunk allowed vlan 6-10
switch(config-if-Et14)#show interfaces ethernet 14 switchport
Name: Et14
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Access Mode VLAN: 1 (inactive)
Trunking Native Mode VLAN: 1 (inactive)
Administrative Native VLAN tagging: disabled
Trunking VLANs Enabled: 6-10
Trunk Groups:

switch(config-if-Et14)#
```

Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 798.

See also Arista User Manual v. 4.12.3 (7/17/13), at 645; Arista User Manual, v. 4.11.1 (1/11/13), at 498; Arista User Manual v. 4.10.3 (10/22/12), at 416; Arista User Manual v. 4.9.3.2 (5/3/12), at 355.

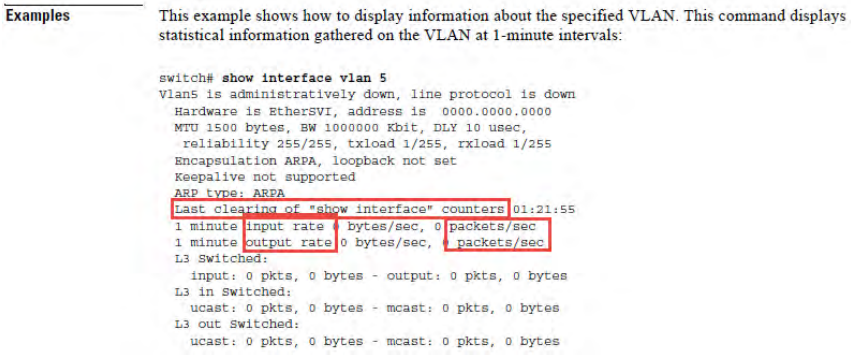
</td>
</tr>
<tr><td></td><td></td><td></td></tr>
</table>

<table>
<tr>
<th>Copyright Registration Information</th>
<th>Cisco</th>
<th>Arista</th>
</tr>
<tr>
<td>

Cisco NX-OS 6.2

Effective date of registration: 11/13/2014

</td>
<td>



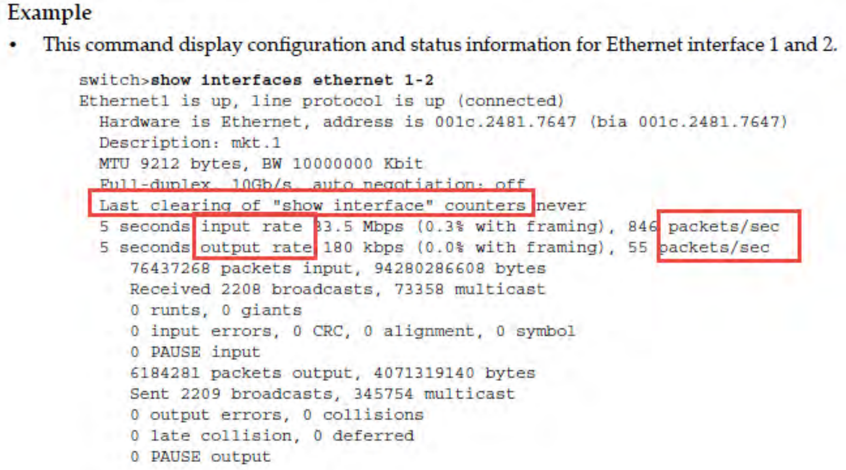
Examples

This example shows how to display information about the specified VLAN. This command displays statistical information gathered on the VLAN at 1-minute intervals:

```
switch# show interface vlan 5
Vlan5 is administratively down, line protocol is down
  Hardware is EtherSVI, address is  0000.0000.0000
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
   reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive not supported
  ARP type: ARPA
  Last clearing of "show interface" counters 01:21:55
  1 minute input rate 0 bytes/sec, 0 packets/sec
  1 minute output rate 0 bytes/sec, 0 packets/sec
  L3 Switched:
    input: 0 pkts, 0 bytes - output: 0 pkts, 0 bytes
  L3 in Switched:
    ucast: 0 pkts, 0 bytes - mcast: 0 pkts, 0 bytes
  L3 out Switched:
    ucast: 0 pkts, 0 bytes - mcast: 0 pkts, 0 bytes
```

Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference (2013), at 49.

</td>
<td>



Example

- This command display configuration and status information for Ethernet interface 1 and 2.

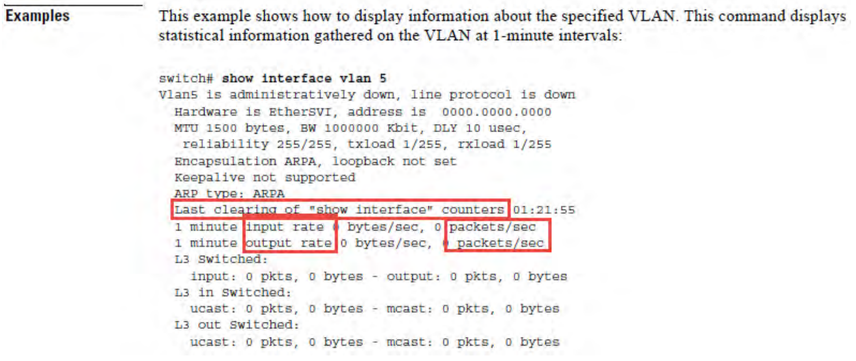
```
switch>show interfaces ethernet 1-2
Ethernet1 is up, line protocol is up (connected)
  Hardware is Ethernet, address is 001c.2481.7647 (bia 001c.2481.7647)
  Description: mkt.1
  MTU 9212 bytes, BW 10000000 Kbit
  Full-duplex, 10Gb/s, auto negotiation: off
  Last clearing of "show interface" counters never
  5 seconds input rate 33.5 Mbps (0.3% with framing), 846 packets/sec
  5 seconds output rate 180 kbps (0.0% with framing), 55 packets/sec
     76437268 packets input, 94280286608 bytes
     Received 2208 broadcasts, 73358 multicast
     0 runts, 0 giants
     0 input errors, 0 CRC, 0 alignment, 0 symbol
     0 PAUSE input
     6184281 packets output, 4071319140 bytes
     Sent 2209 broadcasts, 345754 multicast
     0 output errors, 0 collisions
     0 late collision, 0 deferred
     0 PAUSE output
```

Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 437.

See also Arista User Manual v. 4.12.3 (7/17/13), at 371; Arista User Manual, v. 4.11.1 (1/11/13), at 312; Arista User Manual v. 4.10.3 (10/22/12), at 270; Arista User Manual v. 4.9.3.2 (5/3/12), at 252.

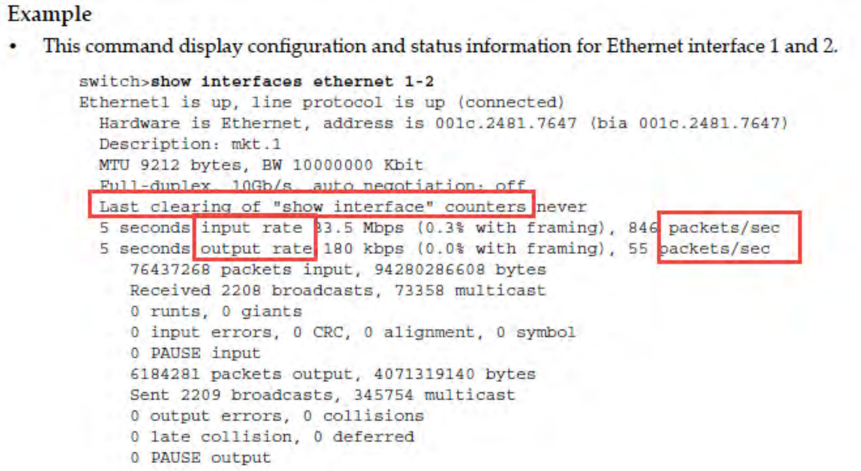
</td>
</tr>
</table>

<table>
<tr><th>Copyright Registration Information</th><th>Cisco</th><th>Arista</th></tr>
<tr>
<td>Cisco NX-OS 5.0

Effective date of registration: 11/13/2014</td>
<td>


Examples This example shows how to display information about the specified VLAN. This command displays statistical information gathered on the VLAN at 1-minute intervals:

<pre>
switch# show interface vlan 5
Vlan5 is administratively down, line protocol is down
  Hardware is EtherSVI, address is 0000.0000.0000
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
   reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive not supported
  ARP type: ARPA
  Last clearing of "show interface" counters 01:21:55
  1 minute input rate 0 bytes/sec, 0 packets/sec
  1 minute output rate 0 bytes/sec, 0 packets/sec
  L3 Switched:
    input: 0 pkts, 0 bytes - output: 0 pkts, 0 bytes
  L3 in Switched:
    ucast: 0 pkts, 0 bytes - mcast: 0 pkts, 0 bytes
  L3 out Switched:
    ucast: 0 pkts, 0 bytes - mcast: 0 pkts, 0 bytes
</pre>

Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference, Release 5.x (2010), at 46.
</td>
<td>


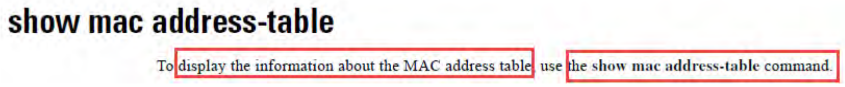
Example

- This command display configuration and status information for Ethernet interface 1 and 2.

<pre>
switch>show interfaces ethernet 1-2
Ethernet1 is up, line protocol is up (connected)
  Hardware is Ethernet, address is 001c.2481.7647 (bia 001c.2481.7647)
  Description: mkt.1
  MTU 9212 bytes, BW 10000000 Kbit
  Full-duplex, 10Gb/s, auto negotiation: off
  Last clearing of "show interface" counters never
  5 seconds input rate 83.5 Mbps (0.3% with framing), 846 packets/sec
  5 seconds output rate 180 kbps (0.0% with framing), 55 packets/sec
     76437268 packets input, 94280286608 bytes
     Received 2208 broadcasts, 73358 multicast
     0 runts, 0 giants
     0 input errors, 0 CRC, 0 alignment, 0 symbol
     0 PAUSE input
     6184281 packets output, 4071319140 bytes
     Sent 2209 broadcasts, 345754 multicast
     0 output errors, 0 collisions
     0 late collision, 0 deferred
     0 PAUSE output
</pre>

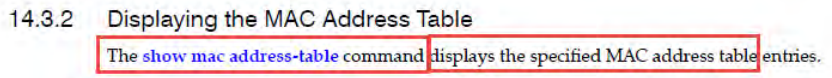
Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 437.

See also Arista User Manual v. 4.12.3 (7/17/13), at 371; Arista User Manual, v. 4.11.1 (1/11/13), at 312; Arista User Manual v. 4.10.3 (10/22/12), at 270; Arista User Manual v. 4.9.3.2 (5/3/12), at 252.
</td>
</tr>
<tr>
<td>Cisco NX-OS 6.2

Effective date of registration: 11/13/2014</td>
<td>


show mac address-table

To display the information about the MAC address table, use the show mac address-table command.

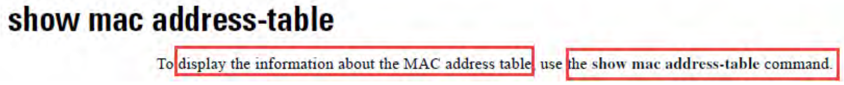
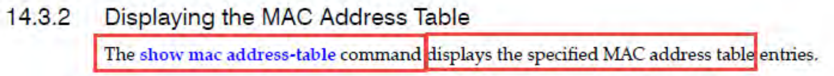
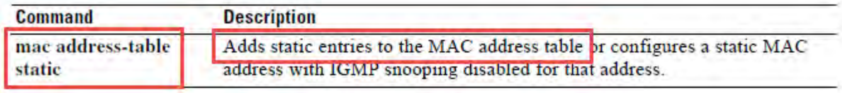
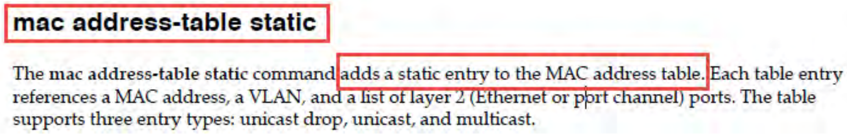
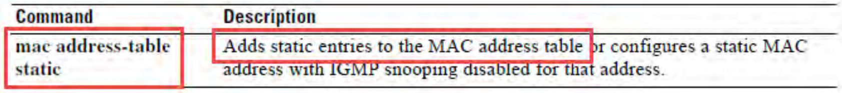
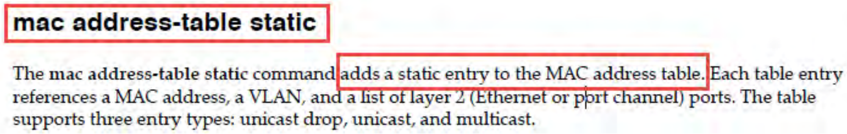
Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference (2013), at 54.
</td>
<td>


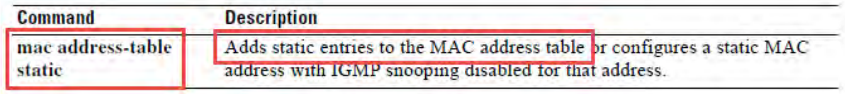
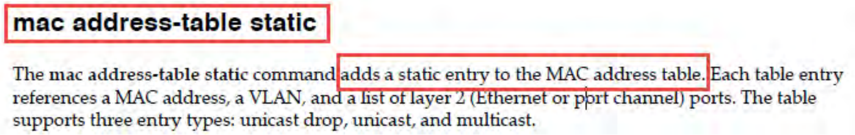
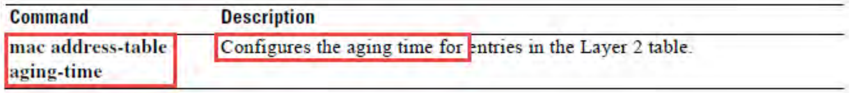
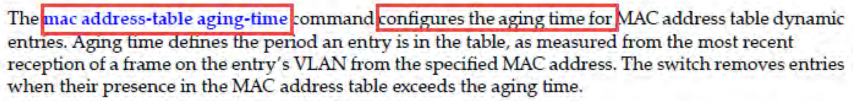
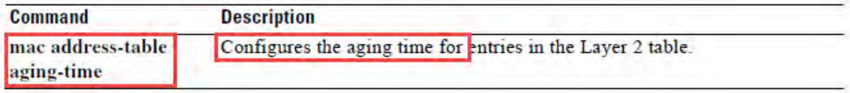
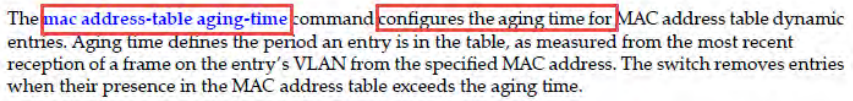
14.3.2 Displaying the MAC Address Table

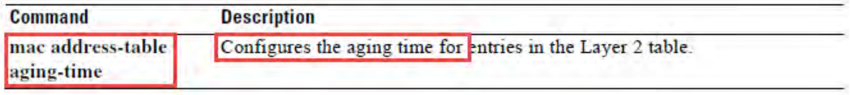
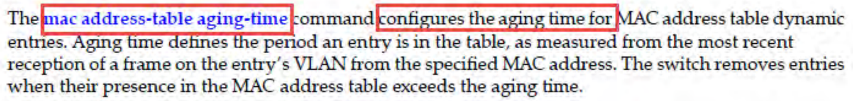
The show mac address-table command displays the specified MAC address table entries.

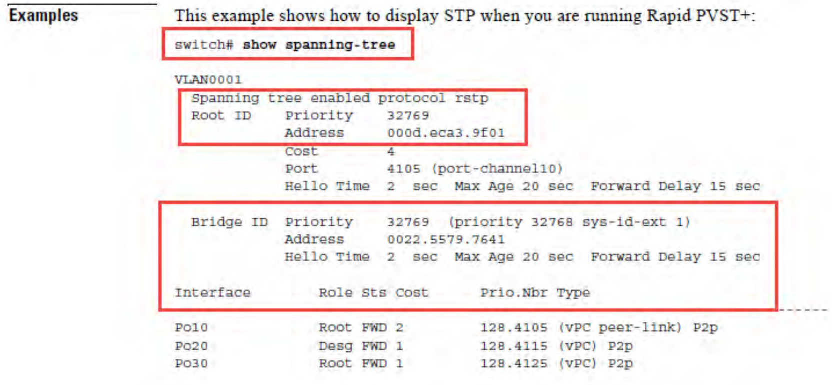
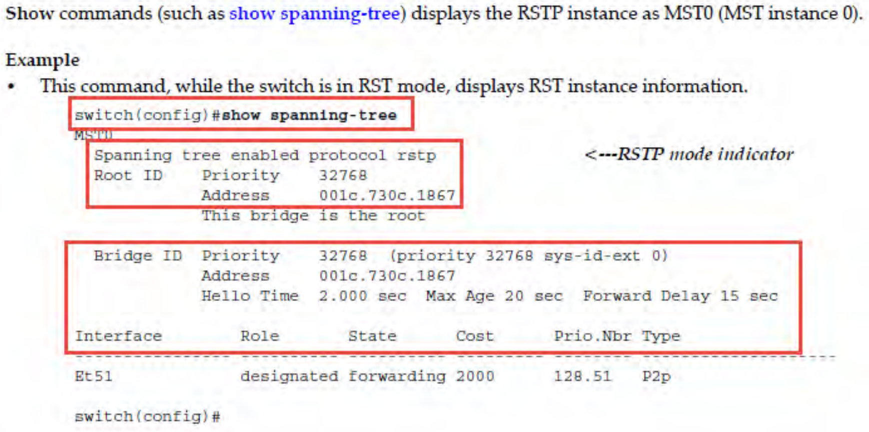
Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 626.

See also Arista User Manual v. 4.12.3 (7/17/13), at 496; Arista User Manual, v. 4.11.1 (1/11/13), at 402; Arista User Manual v. 4.10.3 (10/22/12), at 360; Arista User Manual v. 4.9.3.2 (5/3/12), at 333.
</td>
</tr>
</table>

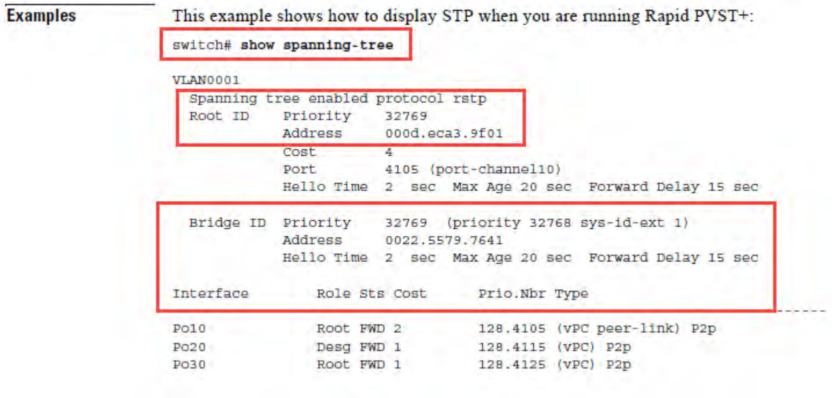
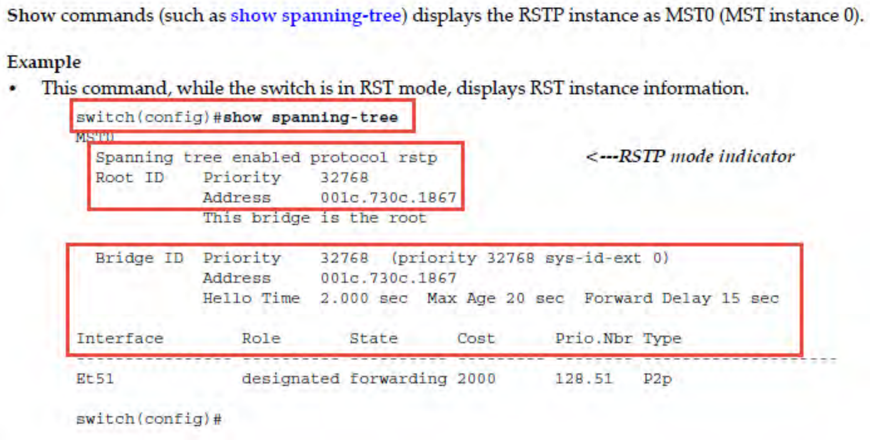
Copyright Registration Information	Cisco	Arista
Cisco NX-OS 5.0 Effective date of registration: 11/13/2014	 **show mac address-table** To display the information about the MAC address table, use the show mac address-table command. Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference (2010), at L-51.	 14.3.2 Displaying the MAC Address Table The show mac address-table command displays the specified MAC address table entries. Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 626. *See also* Arista User Manual v. 4.12.3 (7/17/13), at 496; Arista User Manual, v. 4.11.1 (1/11/13), at 402; Arista User Manual v. 4.10.3 (10/22/12), at 360; Arista User Manual v. 4.9.3.2 (5/3/12), at 333.
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	 **Command** **Description** mac address-table static — Adds static entries to the MAC address table or configures a static MAC address with IGMP snooping disabled for that address. Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference (2013), at 40.	 **mac address-table static** The mac address-table static command adds a static entry to the MAC address table. Each table entry references a MAC address, a VLAN, and a list of layer 2 (Ethernet or port channel) ports. The table supports three entry types: unicast drop, unicast, and multicast. Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 664 *See also* Arista User Manual v. 4.12.3 (7/17/13), at 532; Arista User Manual, v. 4.11.1 (1/11/13), at 427.
Cisco NX-OS 5.0 Effective date of registration: 11/13/2014	 **Command** **Description** mac address-table static — Adds static entries to the MAC address table or configures a static MAC address with IGMP snooping disabled for that address. Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference, Release 5.x (2013), at L2-53.	 **mac address-table static** The mac address-table static command adds a static entry to the MAC address table. Each table entry references a MAC address, a VLAN, and a list of layer 2 (Ethernet or port channel) ports. The table supports three entry types: unicast drop, unicast, and multicast. Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 664 *See also* Arista User Manual v. 4.12.3 (7/17/13), at 532; Arista User Manual, v. 4.11.1 (1/11/13), at 427.

Copyright Registration Information	Cisco	Arista
Cisco IOS 5.1 Effective date of registration: 11/28/2014	 Command Description mac address-table static — Adds static entries to the MAC address table or configures a static MAC address with IGMP snooping disabled for that address. Cisco lOS Security Command Reference (2010), at SEC-2374.	 **mac address-table static** The mac address-table static command adds a static entry to the MAC address table. Each table entry references a MAC address, a VLAN, and a list of layer 2 (Ethernet or port channel) ports. The table supports three entry types: unicast drop, unicast, and multicast. Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 664 *See also* Arista User Manual v. 4.12.3 (7/17/13), at 532; Arista User Manual, v. 4.11.1 (1/11/13), at 427.
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	 Command Description mac address-table aging-time — Configures the aging time for entries in the Layer 2 table. Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference (2013), at 57.	 The mac address-table aging-time command configures the aging time for MAC address table dynamic entries. Aging time defines the period an entry is in the table, as measured from the most recent reception of a frame on the entry's VLAN from the specified MAC address. The switch removes entries when their presence in the MAC address table exceeds the aging time. Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 662 *See also* Arista User Manual v. 4.12.3 (7/17/13), at 496; Arista User Manual, v. 4.11.1 (1/11/13), at 426; Arista User Manual v. 4.10.3 (10/22/12), at 332; Arista User Manual v. 4.9.3.2 (5/3/12), at 320.
Cisco IOS 5.1 Effective date of registration: 11/28/201	 Command Description mac address-table aging-time — Configures the aging time for entries in the Layer 2 table. Cisco lOS Security Command Reference (2010), at SEC-2374.	 The mac address-table aging-time command configures the aging time for MAC address table dynamic entries. Aging time defines the period an entry is in the table, as measured from the most recent reception of a frame on the entry's VLAN from the specified MAC address. The switch removes entries when their presence in the MAC address table exceeds the aging time. Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 662 *See also* Arista User Manual v. 4.12.3 (7/17/13), at 496; Arista User Manual, v. 4.11.1 (1/11/13), at 426; Arista User Manual v. 4.10.3 (10/22/12), at 332; Arista User Manual v. 4.9.3.2 (5/3/12), at 320.

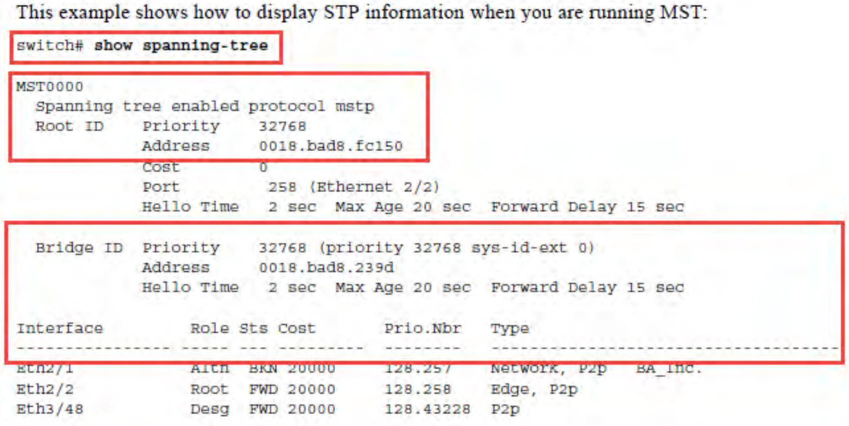
Copyright Registration Information	Cisco	Arista
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	 **Command** — **Description** **mac address-table aging-time** — Configures the aging time for entries in the Layer 2 table. Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference, Release 5.x (2010), at L-54.	 The mac address-table aging-time command configures the aging time for MAC address table dynamic entries. Aging time defines the period an entry is in the table, as measured from the most recent reception of a frame on the entry's VLAN from the specified MAC address. The switch removes entries when their presence in the MAC address table exceeds the aging time. Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 662 *See also* Arista User Manual v. 4.12.3 (7/17/13), at 496; Arista User Manual, v. 4.11.1 (1/11/13), at 426; Arista User Manual v. 4.10.3 (10/22/12), at 332; Arista User Manual v. 4.9.3.2 (5/3/12), at 320.

Cisco NX-OS 6.2
 	
Effective date of registration: 11/13/2014
	
	Examples This example shows how to display STP when you are running Rapid PVST+:
	`switch# show spanning-tree`
	`VLAN0001`
	`  Spanning tree enabled protocol rstp`
	`  Root ID    Priority    32769`
	`             Address     000d.eca3.9f01`
	`             Cost        4`
	`             Port        4105 (port-channel10)`
	`             Hello Time  2  sec  Max Age 20 sec  Forward Delay 15 sec`
	`  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)`
	`             Address     0022.5579.7641`
	`             Hello Time  2  sec  Max Age 20 sec  Forward Delay 15 sec`
	`Interface        Role Sts Cost      Prio.Nbr Type`
	`Po10             Root FWD 2         128.4105 (vPC peer-link) P2p`
	`Po20             Desg FWD 1         128.4115 (vPC) P2p`
	`Po30             Root FWD 1         128.4125 (vPC) P2p`
	
	Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference, (2013), at 63.
		
		Show commands (such as show spanning-tree) displays the RSTP instance as MST0 (MST instance 0).
		
		Example
		• This command, while the switch is in RST mode, displays RST instance information.
		`switch(config)#show spanning-tree`
		`MST0`
		`  Spanning tree enabled protocol rstp` *<---RSTP mode indicator*
		`  Root ID    Priority    32768`
		`             Address     001c.730c.1867`
		`             This bridge is the root`
		`  Bridge ID  Priority    32768  (priority 32768 sys-id-ext 0)`
		`             Address     001c.730c.1867`
		`             Hello Time  2.000 sec  Max Age 20 sec  Forward Delay 15 sec`
		`Interface        Role       State      Cost      Prio.Nbr Type`
		`---------------- ---------- ---------- --------- -------- --------------------`
		`Et51             designated forwarding 2000      128.51   P2p`
		`switch(config)#`
		
		Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 960.
		
		See also Arista User Manual v. 4.12.3 (7/17/13), at 838; Arista User Manual, v. 4.11.1 (1/11/13), at 656; Arista User Manual v. 4.10.3 (10/22/12), at 570; Arista User Manual v. 4.9.3.2 (5/3/12), at 490; Arista User Manual v. 4.8.2 (11/18/11), at 364; Arista User Manual v. 4.7.3 (7/18/11), at 238; Arista User Manual v. 4.6.0 (12/22/2010), at 268.

Copyright Registration Information	Cisco	Arista

Cisco NX-OS 5.0
 	
Effective date of registration: 11/13/2014
	
	Examples This example shows how to display STP when you are running Rapid PVST+:
	`switch# show spanning-tree`
	`VLAN0001`
	`  Spanning tree enabled protocol rstp`
	`  Root ID    Priority    32769`
	`             Address     000d.eca3.9f01`
	`             Cost        4`
	`             Port        4105 (port-channel10)`
	`             Hello Time  2  sec  Max Age 20 sec  Forward Delay 15 sec`
	`  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)`
	`             Address     0022.5579.7641`
	`             Hello Time  2  sec  Max Age 20 sec  Forward Delay 15 sec`
	`Interface        Role Sts Cost      Prio.Nbr Type`
	`------`
	`Po10             Root FWD 2         128.4105 (vPC peer-link) P2p`
	`Po20             Desg FWD 1         128.4115 (vPC) P2p`
	`Po30             Root FWD 1         128.4125 (vPC) P2p`
	
	Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference, Release 5.x (2010), at L59-60.
		
		Show commands (such as show spanning-tree) displays the RSTP instance as MST0 (MST instance 0).
		Example
		• This command, while the switch is in RST mode, displays RST instance information.
		`switch(config)#show spanning-tree`
		`MST0`
		`  Spanning tree enabled protocol rstp`
		`  Root ID    Priority    32768`
		`             Address     001c.730c.1867`
		`             This bridge is the root`
		`  Bridge ID  Priority    32768  (priority 32768 sys-id-ext 0)`
		`             Address     001c.730c.1867`
		`             Hello Time  2.000 sec  Max Age 20 sec  Forward Delay 15 sec`
		`Interface        Role       State      Cost      Prio.Nbr Type`
		`---------------- ---------- ---------- --------- -------- --------------------`
		`Et51             designated forwarding 2000      128.51   P2p`
		`switch(config)#`
		<---RSTP mode indicator
		
		Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 960.
		
		See also Arista User Manual v. 4.12.3 (7/17/13), at 838; Arista User Manual, v. 4.11.1 (1/11/13), at 656; Arista User Manual v. 4.10.3 (10/22/12), at 570; Arista User Manual v. 4.9.3.2 (5/3/12), at 490; Arista User Manual v. 4.8.2 (11/18/11), at 364; Arista User Manual v. 4.7.3 (7/18/11), at 238; Arista User Manual v. 4.6.0 (12/22/2010), at 268.

<table>
<tr><th>Copyright Registration Information</th><th>Cisco</th><th>Arista</th></tr>
<tr>
<td>Cisco NX-OS 6.2
Effective date of registration: 11/13/2014</td>
<td>

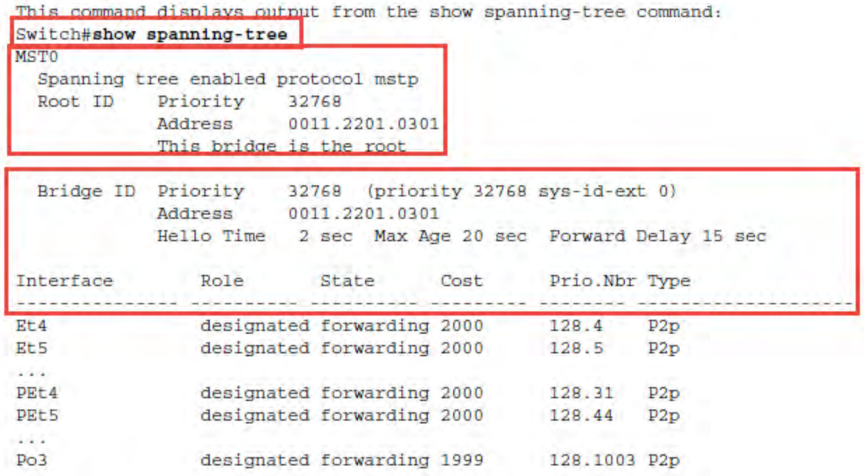


This example shows how to display STP information when you are running MST:

```
switch# show spanning-tree

MST0000
  Spanning tree enabled protocol mstp
  Root ID     Priority     32768
              Address      0018.bad8.fc150
              Cost         0
              Port          258 (Ethernet 2/2)
              Hello Time    2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority     32768 (priority 32768 sys-id-ext 0)
              Address      0018.bad8.239d
              Hello Time    2 sec  Max Age 20 sec  Forward Delay 15 sec

Interface        Role Sts Cost       Prio.Nbr   Type
---------------- ----- --- ---------  --------  ------------------------------------
Eth2/1           Altn  BKN 20000      128.257   Network, P2p   BA_Inc.
Eth2/2           Root  FWD 20000      128.258   Edge, P2p
Eth3/48          Desg  FWD 20000      128.43228 P2p
```

Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference (2013), at 64

</td>
<td>



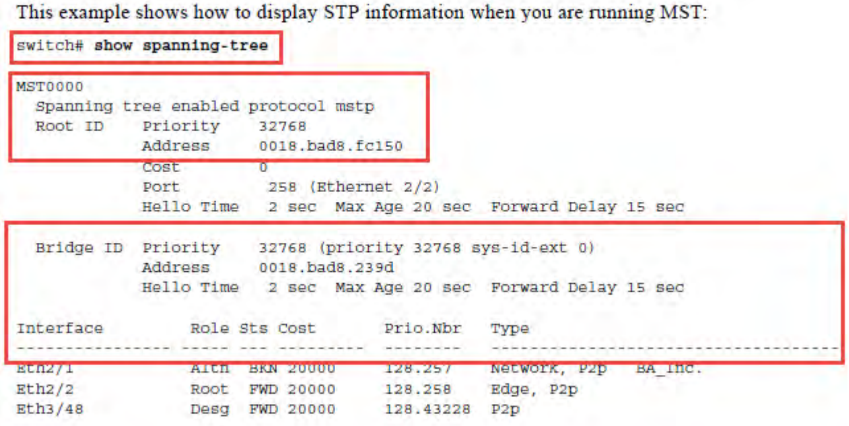
```
This command displays output from the show spanning-tree command:
Switch#show spanning-tree
MST0
  Spanning tree enabled protocol mstp
  Root ID     Priority     32768
              Address      0011.2201.0301
              This bridge is the root

  Bridge ID   Priority     32768  (priority 32768 sys-id-ext 0)
              Address      0011.2201.0301
              Hello Time    2 sec  Max Age 20 sec  Forward Delay 15 sec

Interface        Role       State      Cost      Prio.Nbr Type
---------------- ---------- ---------- --------- -------- --------------------
Et4              designated forwarding 2000      128.4    P2p
Et5              designated forwarding 2000      128.5    P2p
...
PEt4             designated forwarding 2000      128.31   P2p
PEt5             designated forwarding 2000      128.44   P2p
...
Po3              designated forwarding 1999      128.1003 P2p
```

Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 983.

See also Arista User Manual v. 4.12.3 (7/17/13), at 861; Arista User Manual, v. 4.11.1 (1/11/13), at 679; Arista User Manual v. 4.10.3 (10/22/12), at 593; Arista User Manual v. 4.9.3.2 (5/3/12), at 512; Arista User Manual v. 4.8.2 (11/18/11), at 386; Arista User Manual v. 4.7.3 (7/18/11), at 275; Arista User Manual v. 4.6.0 (12/22/2010), at 295

</td>
</tr>
</table>

<table>
<tr><th>Copyright Registration Information</th><th>Cisco</th><th>Arista</th></tr>
<tr>
<td>Cisco NX-OS 5.0
Effective date of registration: 11/13/2014</td>
<td>

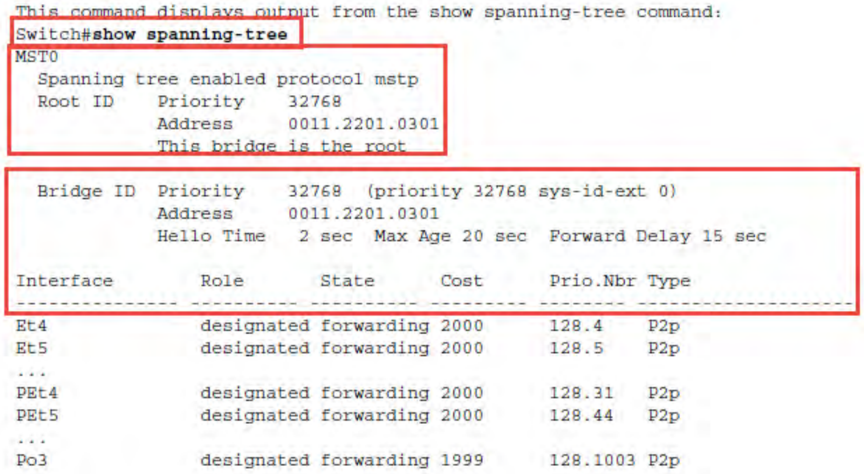


This example shows how to display STP information when you are running MST:

```
switch# show spanning-tree

MST0000
  Spanning tree enabled protocol mstp
  Root ID    Priority    32768
             Address     0018.bad8.fc150
             Cost        0
             Port         258 (Ethernet 2/2)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32768 (priority 32768 sys-id-ext 0)
             Address     0018.bad8.239d
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

Interface        Role Sts Cost      Prio.Nbr  Type
---------------- ----- --- --------- --------  --------------------------------------
Eth2/1           Altn BKN 20000     128.257   Network, P2p  BA_Inc.
Eth2/2           Root FWD 20000     128.258   Edge, P2p
Eth3/48          Desg FWD 20000     128.43228 P2p
```

Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference, Release 5.x (2010), at L2-59:L2-61

</td>
<td>



```
This command displays output from the show spanning-tree command:
Switch#show spanning-tree
MST0
  Spanning tree enabled protocol mstp
  Root ID    Priority    32768
             Address     0011.2201.0301
             This bridge is the root

  Bridge ID  Priority    32768  (priority 32768 sys-id-ext 0)
             Address     0011.2201.0301
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

Interface        Role       State      Cost      Prio.Nbr Type
---------------- ---------- ---------- --------- -------- --------------------
Et4              designated forwarding 2000      128.4    P2p
Et5              designated forwarding 2000      128.5    P2p
...
PEt4             designated forwarding 2000      128.31   P2p
PEt5             designated forwarding 2000      128.44   P2p
...
Po3              designated forwarding 1999      128.1003 P2p
```

Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 983.

See also Arista User Manual v. 4.12.3 (7/17/13), at 861; Arista User Manual, v. 4.11.1 (1/11/13), at 679; Arista User Manual v. 4.10.3 (10/22/12), at 593; Arista User Manual v. 4.9.3.2 (5/3/12), at 512; Arista User Manual v. 4.8.2 (11/18/11), at 386; Arista User Manual v. 4.7.3 (7/18/11), at 275; Arista User Manual v. 4.6.0 (12/22/2010), at 295

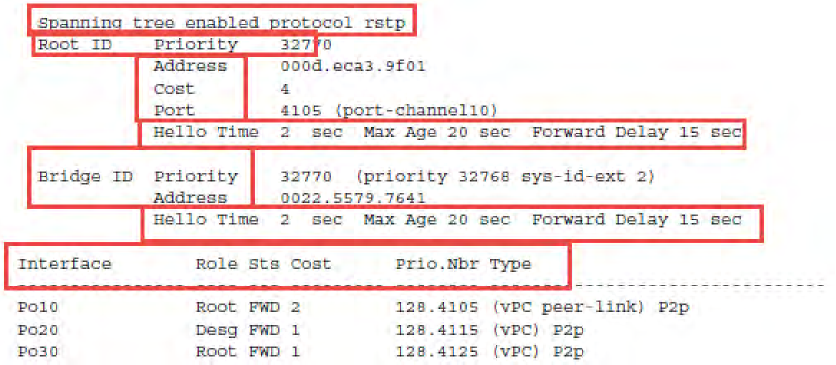
</td>
</tr>
</table>

<table>
<tr><th>Copyright Registration Information</th><th>Cisco</th><th>Arista</th></tr>
<tr>
<td>

Cisco NX-OS 6.2

Effective date of registration: 11/13/2014

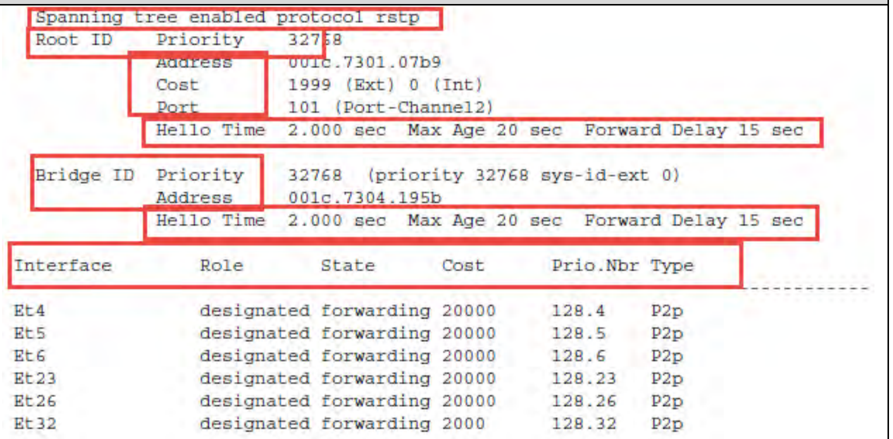
</td>
<td>



```
Spanning tree enabled protocol rstp
Root ID     Priority    32770
            Address     000d.eca3.9f01
            Cost        4
            Port        4105 (port-channel10)
            Hello Time  2  sec  Max Age 20 sec  Forward Delay 15 sec

Bridge ID   Priority    32770  (priority 32768 sys-id-ext 2)
            Address     0022.5579.7641
            Hello Time  2  sec  Max Age 20 sec  Forward Delay 15 sec

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Po10             Root FWD 2         128.4105 (vPC peer-link) P2p
Po20             Desg FWD 1         128.4115 (vPC) P2p
Po30             Root FWD 1         128.4125 (vPC) P2p
```

Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference at 67

</td>
<td>



```
Spanning tree enabled protocol rstp
Root ID     Priority    32768
            Address     001c.7301.07b9
            Cost        1999 (Ext) 0 (Int)
            Port        101 (Port-Channel2)
            Hello Time  2.000 sec  Max Age 20 sec  Forward Delay 15 sec

Bridge ID   Priority    32768  (priority 32768 sys-id-ext 0)
            Address     001c.7304.195b
            Hello Time  2.000 sec  Max Age 20 sec  Forward Delay 15 sec

Interface        Role       State      Cost      Prio.Nbr Type
----------------------------------------------------------------------------
Et4              designated forwarding 20000     128.4    P2p
Et5              designated forwarding 20000     128.5    P2p
Et6              designated forwarding 20000     128.6    P2p
Et23             designated forwarding 20000     128.23   P2p
Et26             designated forwarding 20000     128.26   P2p
Et32             designated forwarding 2000      128.32   P2p
```

Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 983.

See also Arista User Manual v. 4.12.3 (7/17/13), at 861; Arista User Manual, v. 4.11.1 (1/11/13), at 679; Arista User Manual v. 4.10.3 (10/22/12), at 593; Arista User Manual v. 4.9.3.2 (5/3/12), at 512; Arista User Manual v. 4.8.2 (11/18/11), at 386; Arista User Manual v. 4.7.3 (7/18/11), at 275; Arista User Manual v. 4.6.0 (12/22/2010), at 268

</td>
</tr>
</table>